

República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(21) **PI0706880-8 A2**

(22) Data de Depósito: 19/01/2007
(43) Data da Publicação: 12/04/2011
(RPI 2101)



(51) *Int.Cl.:*
G06F 15/16

(54) Título: **SISTEMA E MÉTODO PARA SEGURANÇA DE REDE**

(30) Prioridade Unionista: 20/01/2006 US 60/760,475

(73) Titular(es): Verimatrix, Inc.

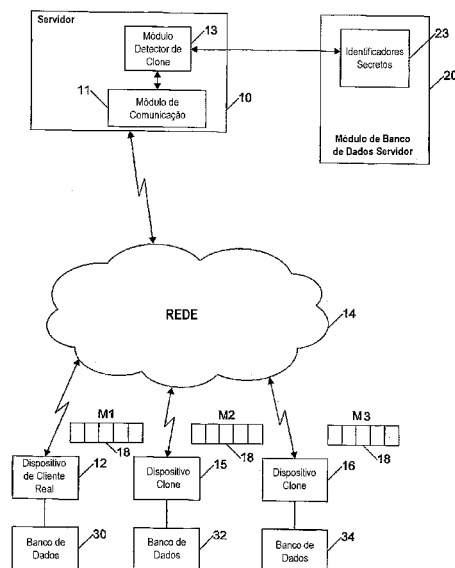
(72) Inventor(es): KULAKOWSKI, ROBERT T.

(74) Procurador(es): PINHEIRO NETO - ADVOGADOS

(86) Pedido Internacional: PCT US2007060744 de 19/01/2007

(87) Publicação Internacional: WO 2007/084973 de 26/07/2007

(57) **Resumo:** SISTEMA E METODO PARA SEGURANÇA DE REDE Em um sistema de segurança para comunicações de rede com dispositivos de cliente, cada dispositivo de cliente tem um módulo de comunicação para se comunicar com pelo menos um servidor em uma rede, um módulo de armazenamento de dados para armazenar um ou mais valores de dados secretos de um ou mais eventos operacionais no dispositivo de cliente, e um módulo gerador de identificador secreto que cria pelo menos um identificador secreto baseado nos valores de dados secretos armazenados. O identificador secreto é provido em uma ou mais mensagens de rede ao servidor, ou caso contrário enviadas ao provedor de serviço, e pode ser provido em resposta a uma requisição específica recebida na rede, ou habitualmente em uma ou mais mensagens normalmente envolvidas em comunicações de rede. O servidor compara os identificadores secretos recebidos de dispositivos de cliente tendo o mesmo identificador de cliente para detectar possíveis clones.



"SISTEMA E MÉTODO PARA SEGURANÇA DE REDE"

Pedido de Patente Relacionado

A presente aplicação reivindica o benefício de pedido de patente provisório co-pendente nos Estados Unidos N° 60/760.475 depositado em 20 de Janeiro de 2006, que é aqui incorporado como referência em sua totalidade.

Campo da Invenção

A presente invenção se relaciona a comunicações de rede entre um servidor e um dispositivo de cliente, e concerne particularmente a um sistema e método de segurança de rede para detectar clones de dispositivos de cliente verdadeiros ou corretamente registrados que tentam roubar serviços sem pagamento ou em todo caso imitar um dispositivo de cliente real.

Estado da Arte Relacionada

Em um ambiente de computação distribuído, piratas tentam roubar serviços criando múltiplos clientes com credenciais idênticas às de um cliente válido ou assinante autorizado, permitindo assim que assinantes não-pagantes compartilhem (roubem) os serviços de um assinante pagante autorizado. Considerando que as credenciais parecem válidas, o servidor envia chaves de radiodifusão ou similar a tais clones, permitindo que assinantes não-autorizados vejam radiodifusões, entrem em comunicações de duas-vias, ou similares. Tais técnicas de clonagem são um problema significativo para provedores de rede. Os piratas também tentam duplicar ou clonar dispositivos de cliente tais como cartões inteligentes que são usados por indivíduos autorizados, tais como cartões de crédito ou de máquinas de caixas eletrônicos automatizados (Banco 24 Horas), em telefones móveis, para identificação de alta segurança e cartões de controle de acesso, cartões de transporte público, e outros propósitos. A clonagem de cartões inteligentes também causas problemas significativos para os provedores de tais serviços bem como aos usuários de cartão autorizados.

Então, o que é preciso é um sistema e método que reduza ou supere estes problemas significativos encontrados nos sistemas convencionais como descrito acima.

Sumário

As formas de incorporação aqui descritas provêm a adição de dados de segurança secretos para mensagens normais entre um dispositivo de cliente e um servidor, de forma que um servidor pode determinar se mais de um dispositivo de cliente comunicando-se com a rede tem as mesmas credenciais registradas ou identificador de cliente (ID de cliente), indicando a presença de um ou mais dispositivos de cliente clonados.

De acordo com um aspecto, é provido um método de segurança para detectar dispositivos de cliente clonados compreendendo receber uma mensagem de um dispositivo de cliente em um servidor, a mensagem contendo um identificador secreto derivado de um ou mais eventos operacionais no dispositivo de cliente, determinando se o identificador secreto coincide com um identificador secreto para o dispositivo de cliente armazenado no servidor, e informando a detecção de um dispositivo de cliente clonado se o identificador secreto não coincidir.

O identificador secreto armazenado no servidor podem ser baseado em um ou mais itens de dados secretos gerados pelo servidor ou pelo dispositivo de cliente, ou ambos, e pode ter sido recebido em uma mensagem prévia que pretende ser do mesmo dispositivo de cliente. Se as mensagens se originam com dispositivos de cliente diferentes, tal como um dispositivo de cliente real e um dispositivo de cliente clonado, os identificadores secretos não coincidem, uma vez que o tempo e os valores de eventos operacionais em um dispositivo de cliente não são idênticos àqueles em outro dispositivo de cliente. O identificador secreto pode ser um valor gerado por, ou baseado em, um ou mais eventos operacionais, por exemplo o momento da ocorrência de um evento ou o número de vezes que um evento particular aconteceu no dispositivo de cliente, ou pode ser uma versão transformada de um ou mais valores de dados secretos usando uma função de adequação de dados ou similar.

O dispositivo de cliente pode ser qualquer tipo de dispositivo computacional capaz de receber e/ou enviar dados em uma rede, tais como caixas de interface (STBs - set top boxes), computadores pessoais, consoles de jogos, telefones celulares, assistentes digitais pessoais (ADPs), equipamentos de vídeo,

cartões inteligentes, e similares. O identificador secreto gerado para o dispositivo de cliente podem compreender um ou mais valores de dados secretos coletados e armazenados por um dispositivo de cliente, ou uma versão transformada de tais valores de dados secretos, e pode ser baseado em qualquer característica operacional ou evento de um dispositivo de cliente que muda com o passar do tempo e que pode ser armazenado pelo dispositivo de cliente, ou pelo dispositivo de cliente e pelo servidor. O identificador secreto podem ser um símbolo ou valor provido pelo servidor, ou pode ser uma combinação de valores de dados secretos gerados pelo cliente e pelo servidor. Uma característica operacional de um dispositivo de cliente conforme aqui referenciado é um evento que ocorre no, ou com relação ao, dispositivo de cliente, e que é único para aquele dispositivo de cliente em particular, tal como um momento no qual um pré-determinado evento operacional ocorre, por exemplo enviando ou recebendo uma mensagem pré-determinada no dispositivo de cliente ou servidor, uma atualização de *firmware*, um tempo de atraso entre enviar uma mensagem à rede e receber uma resposta da rede, o momento quando um enésimo pacote de rede é recebido no dispositivo de cliente, o número de vezes que um certo evento operacional acontece, um símbolo enviado ao dispositivo de cliente a partir do servidor, uma contagem de pacotes de Mensagem de Controle de Entitulação (MCE) recebidos, um canal no qual o dispositivo de cliente foi sintonizado em um pré-determinado momento, número de mudanças de canal em um pré-determinado tempo, um valor de registro contido em um *chip* em um dispositivo de cliente, e assim por diante. No caso de um cartão inteligente, a característica operacional usada para gerar dados secretos pode ser o momento (data/hora) do primeiro uso do cartão inteligente, o tempo em micro-segundos de quando o cartão inteligente foi usado para uma certa operação, o número total de *bytes* de dados processados pelo cartão inteligente em um certo momento ou capturados em um certo evento tal como a ativação de um evento radiodifundido, ou quaisquer outros dados operacionais, contagens, ou evento que acontece durante o uso do cartão inteligente, por exemplo. No caso de um telefone móvel, chamadas de conexão no telefone podem ser

usadas para gerar o identificador secreto, processando a chamada de conexão com uma função de adequação de dados para gerar um identificador que é único para aquele telefone. A característica operacional é aquela que é criada pela operação de um dispositivo de cliente em particular e portanto não é facilmente copiada ou duplicada por um dispositivo de cliente clonado, por exemplo o tempo em micro-segundos do dia em que um evento aconteceu ou em que ocorreu uma ativação de evento, ou em que novos dados foram capturados. Os identificadores secretos podem ser atualizados usando periodicamente novos eventos operacionais para prover os valores de dados secretos, para adicionalmente reduzir o risco de sucesso de cópias piratas.

Alguns exemplos de possíveis valores de dados secretos que podem ser usados para criar um identificador secreto único para um dispositivo de cliente é a última vez em que um tipo de mensagem em particular foi enviada do, ou recebida pelo, dispositivo de cliente, o número de vezes que um evento particular aconteceu, tal como o número de itens comprados, o número de atualizações de chaves de transiente recebidas, o número de vezes que um certo tipo de mensagem de dados ou pacote de rede foi recebido, ou o número de vezes que um dispositivo de cliente executou um certo evento, o endereço do protocolo de internet (PI) usado pelo servidor de Protocolo de Configuração de Hospedeiro Dinâmico (PCHD) quando usado no sistema, valores obtidos de outros dispositivos de rede tal como um modem por fio ou a força do sinal, o valor de um parâmetro de dados de cliente depois que um pré-determinado número de eventos aconteceu, e similares. Um valor de dados secreto pode compreender dados recebidos em uma mensagem do servidor e usados em uma mensagem subsequente para o servidor. Este valor pode ser atualizado pelo servidor a cada comunicação subsequente. Deste modo, o servidor reconhece que há um dispositivo clone em potencial se uma mensagem for recebida sem conter os valores de dados secretos atualizados, isto é, há mais de um dispositivo de cliente com as mesmas credenciais no sistema. Mais de um valor de dados secreto pode ser usado para o identificador secreto em cada mensagem, para maior segurança. No caso de um cartão inteligente, o identificador secreto pode ser

baseado no momento em que o cartão foi usado, no número de itens comprados, ou similares.

Ativadores de eventos podem ser usados em algumas formas de incorporação para atualizar ou modificar valores de dados secretos ou começar uma contagem ou temporização que resulta em valores de dados secretos atualizados usados para gerar um novo identificador secreto, ou modificar os dados ou protocolo de mensagens contidos em uma mensagem entre um cliente e servidor.

Em outro aspecto, é provido um sistema de segurança para detectar dispositivos de cliente clonados, compreendendo um módulo de armazenamento de dados de servidor de rede que armazena uma pluralidade de conjuntos de credenciais de cliente ou identificadores de cliente (ID) para uma pluralidade de dispositivos de cliente autorizados ou reais, e também armazena identificadores secretos baseados em características operacionais de um dispositivo de cliente que são recebidas em mensagens de dispositivos de cliente, e um módulo de processamento de dados secretos que compara um identificador secreto em uma mensagem recebida de um dispositivo de cliente com um identificador secreto previamente armazenado correspondendo ao mesmo ID de cliente e que cria um relatório de detecção de clone se os identificadores de dados secretos não coincidirem.

Se a rede for uma rede de duas-vias, os identificadores secretos baseados em eventos operacionais coletados são trocados durante comunicações de rede normais. Se a rede normalmente opera como uma rede de uma só via mas tem um canal de retorno para certas comunicações de cliente, valores de dados secretos pré-determinados baseados no uso do dispositivo são coletados e usados para criar identificadores secretos armazenados por dispositivos de cliente. O identificadores secretos são enviados ao servidor em mensagens pelo canal de retorno quando disponível, por exemplo durante um processo de renovação periódica. O servidor armazena o primeiro identificador secreto para um certo assinante. Se um identificador secreto for mais tarde recebido pretendendo se originar com o mesmo dispositivo de cliente, um relatório de detecção de clone é emitido pelo servidor.

De acordo com outro aspecto, é provido um dispositivo de cliente que compreende um módulo gerador de dados secretos para gerar um identificador secreto baseado em dados gerados pela operação do dispositivo de cliente, e um módulo de armazenamento de dados secretos para armazenar o identificador secreto. Se for planejado que o dispositivo de cliente é para uso em um ambiente de rede de duas-vias, ou em um ambiente de rede de uma-via incluindo um canal de retorno para certas comunicações, o dispositivo de cliente também pode incluir um módulo gerador de mensagem para gerar mensagens contendo o identificador secreto atualmente armazenado. O identificador secreto é enviado subsequente a um servidor de rede em uma rede em um campo de dados secretos embutido em uma mensagem, ou como um valor de dados em resposta a uma requisição do servidor ou qualquer combinação relacionada. A mensagem pode ser um tipo de mensagem normalmente enviada em comunicações de duas-vias para uma rede, ou em uma mensagem como parte de um procedimento de renovação periódica ou outra mensagem padrão se o dispositivo de cliente normalmente está envolvido somente em comunicações de uma-via com uma rede.

Onde não há canal de retorno para um serviço de rede de uma-via, o dispositivo de cliente cria e armazena um identificador de cliente que pode ser atualizado periodicamente baseado em novos eventos no dispositivo de cliente. O dispositivo de cliente ou um servidor de rede pode incluir um módulo gerador de código de serviço que gera uma mensagem de código de serviço em um dispositivo de cliente a intervalos pré-determinados. Esta mensagem pode pedir para os assinantes chamarem um centro de serviço ou enviar uma mensagem de texto de serviço de mensagem curta (SMC), por meio de um telefone móvel ou conexão de internet, para o centro de serviço, provendo a identificação de assinante e o identificador secreto atualmente armazenado no dispositivo de cliente. Considerando que o identificador secreto atualmente armazenado é diferente para um dispositivo de cliente real e um dispositivo de cliente clonado, porque eles foram operados diferentemente, o centro de serviço pode determinar quando duas mensagens foram recebidas com a mesma identificação de cliente ou assinante mas com identificadores secretos diferentes. O centro de

serviço pode então usar etapas adicionais para determinar qual dispositivo de cliente está associado com o assinante autorizado, e renova somente aquele dispositivo de cliente, cortando o serviço para qualquer outro dispositivo de cliente usando a mesma
5 identificação de assinante ou cliente.

O identificador secreto é gerado por eventos operacionais que acontecem durante a operação real de um dispositivo de cliente. Porque os eventos operacionais ocorrem depois da fabricação do dispositivo de cliente e são baseados em
10 como os assinantes usam os dispositivos de cliente, os eventos operacionais são únicos para um dispositivo de cliente em particular. Estes eventos operacionais são diferentes mesmo entre dispositivos de cliente clonados, porque dispositivos de cliente clonados fazem as coisas diferentemente depois que eles são
15 acionados, e é esta diferença de operação que é usada para gerar o identificador secreto. Os dados secretos então provêm um identificador único para um dispositivo de cliente em particular, que é armazenado pelo dispositivo de cliente e subseqüentemente usado em mensagens para um servidor. Onde o dispositivo de cliente
20 é normalmente usado somente em comunicações de rede de uma-via, o identificador secreto único pode ser provido à rede em um procedimento de renovação periódica, ou pode ser requisitado por um servidor de rede se houver suspeita de clonagem.

O módulo gerador de dados secretos pode ser
25 incorporado em uma unidade de processamento central do dispositivo de cliente, que pode estar embutida em um único *chip* (sistema em um *chip* ou SUC) em alguns casos, tal como em um cartão inteligente, telefone celular, ou similar. O módulo de armazenamento de dados secreto também pode ser incorporado na
30 unidade de processamento central (UPC) ou em um banco de dados separado associado com a unidade de processamento central, ou em uma memória interna ou externa à UPC.

Um formato de mensagem de dispositivo de cliente em uma forma de incorporação compreende um campo de identificador
35 de mensagem, um campo de dados secretos, e pelo menos um campo de dados adicional contendo a mensagem a ser comunicada ao servidor, tal como um campo de identificação de cliente ou requisição de

chave, ou como parte de uma mensagem ou ID de mensagem. O tipo de mensagem pode ser uma mensagem de inscrição/entrada (*logon*), uma mensagem de requisição de chave de radiodifusão, uma mensagem de compra por comércio eletrônico, uma requisição para troca de canais, uma mensagem de renovação de assinatura, ou similar. Se o tipo de mensagem for uma mensagem de inscrição, os campos de dados adicionais contêm o nome e senha de usuário. O campo de dados secreto contém um identificador secreto que pode compreender um ou mais valores de dados secretos ou itens ou uma versão transformada de tais valores de dados secretos. O identificador secreto pode ser usado pelo servidor na recepção da mensagem para determinar se mais de um dispositivo de cliente está usando as mesmas credenciais. Mais de um tipo de mensagem pode conter um identificador secreto.

Em uma forma de incorporação, o identificador secreto atual é enviado a um servidor a partir de um dispositivo de cliente como parte de mensagens normais tais como conexão em um sistema, requisição de uma chave de decriptação, execução de uma transação de comércio eletrônico, ou outras mensagens e eventos que acontecem normalmente dentro de um sistema. Valores de dados secretos usados para criar o identificador secreto podem ser baseados em vários eventos, e ativadores de eventos podem ser usados para definir eventos que ativam a atualização ou modificação de um identificador secreto previamente armazenado. Identificadores secretos adicionados nas mensagens normais entre um cliente e servidor não requerem mensagens adicionais ou reconhecimentos adicionais entre o cliente e o servidor, reduzindo a probabilidade de um *hacker* (pirata) poder monitorar o protocolo e determinar como copiar um sistema. Como tal, um *hacker* que está tentando roubar serviços através da clonagem de credenciais de assinante, por exemplo, de uma caixa de interface (STB), também precisa ter conhecimento do significado do identificador secreto e dos ativadores que causam uma mudança no identificador secreto para assegurar que STBs autênticas e STBs clonadas tenham o mesmo identificador secreto. Mais de um valor de dados secreto pode ser usado para criar identificadores secretos, por exemplo uma biblioteca de cliente de dois ou mais valores de dados secretos

pode ser usada para criar identificadores secretos em cada mensagem de cliente selecionada para um servidor. A biblioteca de cliente de valores de dados secretos é atualizada periodicamente, tornando mais difícil ocultar dispositivos clonados de um servidor. Em formas de incorporação alternativas, o identificador secreto pode ser enviado também com mensagens separadas entre o cliente e servidor.

O sistema de segurança também pode incluir um processo de renovação projetado para identificar dispositivos de clone suspeitos. O processo de renovação pode ser iniciado em resposta a um relatório de detecção de clone gerado por um servidor de rede, ou pode ser executado a intervalos periódicos ou quando há suspeita de clones por outras razões. O processo de renovação é projetado para re-autorizar somente um único dispositivo de cliente quando vários de tais dispositivos estiverem usando as mesmas credenciais.

Outras características e vantagens da presente invenção ficarão mais prontamente aparentes para aqueles com habilidades comuns na arte depois de revisarem a seguinte descrição detalhada e os desenhos anexos.

Breve Descrição dos Desenhos

Os detalhes da presente invenção, tanto sobre sua estrutura como sobre sua operação, podem ser observados em parte através do estudo dos desenhos acompanhantes, onde os mesmos números de referência se referem às mesmas partes, e nos quais:

A figura 1 é um diagrama de blocos ilustrando uma rede com um dispositivo de cliente real ou autorizado e alguns dispositivos de cliente clonados que se comunicam com um servidor em uma forma de incorporação de um sistema de segurança para detectar dispositivos de cliente clonados em potencial;

A figura 2A é um diagrama que ilustra campos de dados em uma mensagem de inscrição e conexão de usuário do estado da arte anterior;

A figura 2B é um diagrama ilustrando campos de dados em uma incorporação de uma mensagem de usuário contendo um identificador secreto usado no servidor em uma forma de

incorporação de um sistema para detectar dispositivos de cliente clonados em potencial;

A figura 3 é um diagrama de blocos que ilustra um dispositivo de cliente configurado para inserir um identificador secreto em mensagens, de acordo com uma forma de incorporação;

A figura 4 é um diagrama de fluxo ilustrando uma forma de incorporação de um método de detectar um dispositivo de cliente clonado;

As figuras 5A e 5B são diagramas de fluxo que ilustram uma forma de incorporação do método de detecção de clone;

As figuras 6A a 6F ilustram mensagens geradas em várias fases no método das figuras 5A e 5B;

A figura 7 é um diagrama de fluxo ilustrando uma forma de incorporação de um método para inserir identificadores secretos em mensagens entre um dispositivo de cliente e um servidor;

A figura 8 é um diagrama de fluxo que ilustra uma forma de incorporação de um método de renovação de serviço usando identificadores secretos; e

A figura 9 é um diagrama de fluxo ilustrando uma modificação do método da figura 8 para uso em um ambiente de rede de uma- via que não tem um canal de retorno de um dispositivo de cliente.

Descrição Detalhada

Certas formas de incorporação como aqui descritas provêm detecção de mais de um dispositivo de cliente usando credenciais idênticas. Por exemplo, um método e sistema como aqui descritos permitem a detecção de dispositivos-clone em potencial usando um identificador secreto baseado em valores de eventos operacionais específicos para um dispositivo de cliente que é adicionado nas mensagens normais entre um dispositivo de cliente e um servidor.

Depois desta descrição ser lida ficará aparente para aqueles qualificados na arte como implementar a invenção em várias formas de incorporação alternativas e aplicações alternativas. Porém, embora várias formas de incorporação da presente invenção sejam aqui descritas, é compreendido que estas

formas de incorporação somente são apresentadas como formas de exemplos, e não de limitação. Como tal, esta descrição detalhada de várias formas de incorporação alternativas não deve ser interpretada como limitante do escopo ou extensão da presente invenção conforme apresentado nas reivindicações anexas.

Na seguinte descrição, um dispositivo de cliente pode ser qualquer tipo de dispositivo capaz de computar e receber dados de uma rede, tal como uma caixa de interface (STB), um computador pessoal, console de jogo, telefone celular, assistente digital pessoal (ADP), reproduutor de mídia pessoal, um equipamento de vídeo tal como um receptor de vídeo digital (RVD), um reproduutor de disco de vídeo digital (DVD), um reproduutor de disco compacto (CD - *compact disc*), um cartão inteligente, ou similares. Um dispositivo de cliente autêntico ou real é o dispositivo que é apropriadamente registrado com o servidor para receber serviços em uma rede, ou serviços locais tais como transações bancárias, compras, e similares autorizadas por uma rede, como no caso de um cartão inteligente. Um dispositivo de cliente clonado é um dispositivo que tem credenciais idênticas às de um dispositivo de cliente real corretamente registrado para serviço na rede, e que é usado por um usuário sem autorização ou não-pagante em uma tentativa de obter dinheiro ou serviços sem autorização. Os termos "dados secretos", "valor de dados secretos" e "ítem de dados secretos" são usados para indicar valores de dados únicos baseados em características operacionais de um dispositivo de cliente, por exemplo valores criados pela operação de um dispositivo de cliente particular ou comunicação daquele dispositivo com um servidor, ou em símbolos ou valores baseados na operação de um dispositivo de cliente que são criados pelo servidor e embutidos em mensagens ao dispositivo de cliente. Tais valores são secretos porque a sua natureza torna difícil que os piratas (*hackers*) os descubram e os dupliquem em dispositivos clonados de cliente, e porque os dados são gerados após a fabricação. O termo "identificador secreto" indica um identificador único para um dispositivo de cliente específico que é gerado baseado em valores de dados secretos associados com a operação daquele dispositivo, e podem compreender um ou mais valores de dados secretos reais em algumas formas de

incorporação, ou pode ser uma versão transformada de tais valores de dados usando uma função de adequação de dados (*hash*) ou de escolha de um valor de número arbitrário, ou executando alguma outra transformação nos dados. O termo "ativador de evento" é usado para indicar eventos que ativam a atualização ou modificação do identificador secreto contido em um protocolo de mensagem entre um dispositivo de cliente e o servidor. Um "contador de eventos" conta eventos executados por um dispositivo de cliente, e pode ser usado como um ativador de evento quando o número de eventos contados excede um limiar.

A figura 1 é um diagrama de blocos de um sistema de segurança de rede que incorpora detecção de clone de acordo com uma forma de incorporação na qual um servidor 10 se comunica com um dispositivo de cliente real ou autorizado 12 em uma rede 14, e vários dispositivos de cliente clonados 15, 16 usando credenciais de cliente idênticas também enviam mensagens ao servidor 10 na rede 14. Um, dois ou mais dispositivos-clone podem tentar usar serviços de rede em qualquer momento posando como um dispositivo de cliente 12. Os piratas de ambiente computacional tentam freqüentemente roubar a rede e outros serviços criando múltiplos clientes com credenciais idênticas, permitindo assim que assinantes não-pagantes compartilhem ou se apropriem dos serviços de um assinante pagante autorizado.

Conforme ilustrado na figura 1, o servidor 10 é conectado ao banco de dados (BD) servidor 20 o qual tem um módulo de armazenamento de dados 23 para armazenar identificadores secretos que podem ser recebidos de dispositivos de cliente em mensagens e/ou gerados pelo servidor. Como visto acima, cada identificador secreto é baseado em eventos operacionais em um dispositivo de cliente específico. O servidor 10 tem um módulo de comunicação 11 que controla as comunicações de rede e um módulo de detecção de clone 13 que compara identificadores secretos em mensagens recebidas de dispositivos de cliente com identificadores secretos previamente armazenados no módulo 21, como descrito abaixo em mais detalhes. O servidor 10 tem módulos adicionais de controle e de processamento de servidor padrão, que não estão ilustrados.

No sistema da figura 1, o dispositivo de cliente 12 envia uma mensagem M1 para o servidor 10, enquanto os dispositivos-clone 15, 16 enviam mensagens semelhantes M2 e M3 ao servidor. Estas mensagens podem ser enviadas em qualquer seqüência, e o servidor é adaptado para detectar a presença de um ou mais clones potenciais apesar da ordem de transmissão das mensagens M1 a M3. Cada mensagem é adaptada para incluir um identificador secreto 18 embutido em uma porção ou campo de dados secretos pré-determinados da mensagem. Os identificadores secretos para dispositivos de cliente que se comunicam com o servidor estão associados com as credenciais de cliente para um dispositivo de cliente e armazenados em um módulo de armazenamento de dados secretos 23 para comparação com futuros identificadores secretos recebidos de um ou mais dispositivos de cliente tendo as mesmas credenciais, como descrito abaixo em mais detalhes. Cada dispositivo de cliente verdadeiro e clonado tem um banco de dados ou armazenamento de memória (RAM, ROM, FLASH, EEPROM) ou armazenamento de registro 30, 32, 34, respectivamente, no qual os valores de dados secretos são armazenados e atualizados nos ativadores de evento pré-determinados. Embora o banco de dados seja mostrado separado do dispositivo de cliente na figura 1, ele pode ficar alojado no dispositivo de cliente ou pode ser parte de uma unidade ou sistema de processamento central em um *chip* (SUC) no dispositivo de cliente, ou na memória do dispositivo tal como uma memória RAM, uma memória *Flash*, uma Memória Segura, e similares.

Um dispositivo de cliente (real ou clonado) 12, 15, ou 16 está ilustrado em mais detalhes na figura 3. O dispositivo de cliente pode ser qualquer dispositivo de cliente configurado para comunicação em uma rede, tal como uma caixa de interface, um computador pessoal, console de jogo, telefone móvel, ADP, reproduutor de mídia portátil, reproduutor de DVD, RVD, ou um cartão inteligente, ou similares. O dispositivo de cliente tem um módulo de armazenamento de dados 30, 32, 34 associado que é mostrado separadamente mas pode ser incorporado no mesmo alojamento com outros módulos do dispositivo de cliente, ou no mesmo *chip* com os outros módulos em alguns casos. O dispositivo de

cliente também tem um módulo de comunicação 17 para controlar as comunicações de rede com o servidor 10, um módulo gerador de identificador secreto 19 para criar identificadores secretos baseado em valores de dados secretos, ativadores de eventos ou dados recebidos do servidor, e um módulo formatador de mensagem 28. Os dispositivos de cliente também incluem módulos de processamento e controle do dispositivo de cliente padrão que não estão ilustrados na figura 3. O módulo de armazenamento de dados tem um módulo de tabela de dados secretos 29 para armazenar a configuração atual de valores de dados secretos, conforme descrito abaixo. Onde o identificador secreto é uma versão transformada dos valores de dados secretos, o identificador secreto atual ou matriz de valores de dados secretos ou grupo de valores de dados secretos também é armazenado no módulo 29.

Em uma forma de incorporação, o módulo formatador de mensagem 28 é adaptado para inserir ou embutir o identificador secreto atual em um ou mais tipos de mensagens enviadas ao servidor. Em outra forma de incorporação na qual o dispositivo de cliente é usado apenas para receber comunicações de rede de uma só via e não tem acesso a um canal de retorno para a rede, o módulo formatador de mensagem 28 é eliminado e o módulo gerador de identificador secreto é configurado para exibir o identificador secreto atualmente armazenado na forma de um código de identificação único para o usuário do dispositivo de cliente com relação a um processo periódico de renovação de assinante, como descrito abaixo em mais detalhes com relação à figura 9.

Em uma forma de incorporação, os dados de segurança secretos ou identificador 18 são baseados em características operacionais do dispositivo a partir do qual a mensagem é transmitida. Tais características são difíceis ou impossíveis de duplicar em um clone do dispositivo de cliente, uma vez que dispositivos de cliente clonados não são operados identicamente para dispositivos de cliente autênticos ou reais, e eventos operacionais tais como mensagens, atualizações, e similares acontecem em momentos diferentes em dispositivos diferentes. Obter eventos idênticos em micro-segundos em dispositivos de cliente do mundo real é quase impossível. Uma

característica operacional de um dispositivo de cliente é um valor único para aquele dispositivo de cliente específico que é gerado baseado na operação do dispositivo de cliente, tal como um momento no qual um evento operacional pré-determinado ocorre, por exemplo enviando ou recebendo uma mensagem pré-determinada no dispositivo de cliente ou servidor, uma atualização de *firmware*, um tempo de atraso entre o envio de uma mensagem à rede e a recepção de uma resposta na rede, o momento em que o enésimo pacote de rede é recebido no dispositivo de cliente, o número de vezes que um dispositivo de cliente executa um certo evento operacional em um período de tempo selecionado, um símbolo enviado ao dispositivo de cliente a partir do servidor, uma contagem de pacotes de MCE recebidos, um canal em que o dispositivo de cliente foi sintonizado em um pré-determinado momento, o número de mudanças de canal em um tempo pré-determinado, um valor de registro contido em um *chip* em um dispositivo de cliente em um certo momento, e assim por diante. Isto demonstra que há um número ilimitado de valores de dados operacionais que podem ser usados para valores de dados secretos gerados (ou valores de dados únicos para a operação de um cliente) porque o valor de dados exato não é importante, mas o que importa é que a probabilidade do valor de dados ser diferente baseado na operação de dois dispositivos idênticos é grande. Se dois ou mais dispositivos de cliente usando as mesmas credenciais estiverem se comunicando na rede, tais características operacionais não são idênticas de um dispositivo de cliente para o outro, e são criadas exclusivamente pela operação de um dispositivo de cliente particular por um usuário. Tais características operacionais e os identificadores secretos baseados em tais características não podem ser pirateados ou duplicados facilmente por um dispositivo de cliente clonado. É improvável que os operadores de dispositivos de cliente clonados possam obter tais características do dispositivo de cliente verdadeiro ou autêntico, e normalmente nem mesmo saberiam quais características operacionais específicas são usadas para criar o identificador secreto, e em uma forma de incorporação os valores de dados secretos mudam entre versões diferentes do *software* do cliente.

O servidor extrai o identificador secreto recebido em uma mensagem de um dispositivo tendo certas credenciais, e compara este identificador com aqueles recebidos em mensagens prévias aparentemente do mesmo dispositivo. Se não
5 houver coincidência, é provável que um ou mais clones estão sendo usados, e o servidor pode prover uma notificação apropriada de provável detecção de clone ao operador do sistema, para ações adicionais. Considerando que o servidor não pode determinar quais dos vários dispositivos de cliente com credenciais idênticas
10 enviando mensagens são dispositivos clonados, o serviço requisitado é provido aos dispositivos, além da notificação de detecção de clone ao operador.

Em uma forma de incorporação, um identificador secreto é transmitido em mensagens comuns trocadas entre o cliente
15 e o servidor. Por exemplo, assuma-se que o cliente precisa entrar em um sistema e uma mensagem de entrada é definida. A mensagem de entrada padrão compreende um nome de usuário e uma senha. Em uma forma de incorporação, a mensagem de entrada inclui um identificador secreto 18 além do nome de usuário e senha. Quando o
20 dispositivo de cliente tenta entrar em um sistema, o dispositivo de cliente provê uma informação de entrada padrão tal como o nome de usuário e senha e o identificador secreto é embutido na mensagem de entrada (ou qualquer mensagem, ou em todas as mensagens) formando um comando de entrada que compreende o
25 identificador secreto como parte da mensagem de entrada padrão. A mensagem de entrada contém o nome de usuário, senha, e bytes de dados adicionais contendo o identificador secreto. Em uma forma de incorporação, os itens ou valores de dados contidos no identificador secreto ou usados para gerar o identificador secreto
30 mudam em momentos diferentes com base em eventos operacionais dentro do cliente, ou mudam baseado na hora do dia, ou baseado em um período de tempo que decorre depois de um certo evento, de modo que o identificador secreto pode ser atualizado mudando os valores de dados secretos em um momento particular ou acrescentando novos
35 itens de dados secretos a itens de dados secretos prévios, em essência aumentando o número de itens de dados secretos para um cliente particular.

Qualquer troca de mensagens padrão entre um dispositivo de cliente e o servidor pode ser usada para detectar clones, tal como uma mensagem de entrada inicial. Um identificador secreto pode ser combinado com mensagens normais e/ou eventos tais como quando um cliente entra em um sistema. Além da informação tipicamente encontrada em um procedimento de entrada, tais como o nome de usuário de cliente e a senha, o identificador secreto pode ser acrescentado à mensagem de entrada que é específica para a operação de um certo dispositivo de cliente, tal como a última vez em que o usuário entrou na rede ou a diferença de tempo entre o procedimento de entrada atual e o de entrada anterior. Os dados secretos podem ser aplicados a todas as mensagens em um sistema de comunicação ou somente a mensagens selecionadas, tal como a mensagem de entrada ou outros tipos de mensagens.

A figura 2A ilustra um protocolo de mensagem de entrada convencional conforme usado atualmente. Esta mensagem compreende um campo de identificador de mensagem (ID) 21 que define o tipo de mensagem dentre um grupo de mensagens suportadas no sistema e que é tipicamente único para cada mensagem em um sistema. Ela também pode incluir um campo de número de sequência opcional 22 que contém um número único para cada mensagem de qualquer tipo no sistema, e é tipicamente uma contagem incremental que permite que o sistema elimine ataques de repetição de mensagens verificando se o número de sequência é novo antes de processar a mensagem. Quando a mensagem for uma mensagem de entrada inicial, ela também tem um campo de nome de usuário 24 que contém o nome do usuário para um usuário, ou dispositivo de cliente no sistema registrado para o serviço ou associado com uma conta de assinante com o provedor de serviço, e um campo de senha 25 que contém a senha para o usuário associado com uma conta ou serviço. A senha é provida quando o usuário ou assinante assina ou se registra com o sistema ou provedor de serviço pela primeira vez, e é verificada pelo servidor em requisições de serviço subsequentes pelo usuário. Os serviços podem ser acessados ou o usuário pode comprar itens usando o serviço somente depois que a senha é provida corretamente em sistemas protegidos por senha. Além disso, os dados secretos podem ser usados como parte da

falsificação da senha para cada cliente com o lado do servidor ficando ciente dos dados secretos para falsificar a senha ou dados, ou o lado do servidor descarregando dados da chave de encriptação ou da chave de falsificação no cliente. Tais senhas às vezes são obtidas por *hackers* (piratas) e usadas em conjunção com dispositivos-clone na tentativa de obter serviços sem pagamento.

A figura 2B ilustra uma forma de incorporação de uma mensagem de entrada inicial modificada que contém um identificador secreto no campo de dados secretos 18 na estrutura de mensagem de entrada regular. O campo de ID, o campo de número de sequência 22, de nome de usuário 24, e de senha 25 são idênticos aos campos correspondentes da figura 2A, mas a mensagem é modificada para prover um identificador secreto em um campo de dados 18 entre os campos 22 e 24. Os campo de dados secretos 18 pode ser provido em outros locais na mensagem em outras formas de incorporação, e pode ser provido em tipos diferentes de mensagens tais como mensagens de requisição de chave de radiodifusão, mensagens de compra de comércio eletrônico, mensagens de troca de canal, e similares. O identificador secreto pode ser provido em apenas um tipo específico de mensagem entre um dispositivo e o servidor, ou pode ser provido em cada mensagem enviada pelo dispositivo, ou intermitentemente em mensagens variadas. A transmissão intermitente de identificadores secretos pode tornar tais identificadores mais difíceis de rastrear através por potenciais *hackers*. Porque as mensagens codificadas são sempre mais seguras do que as mensagens não-encriptadas entre o cliente e o servidor, em uma forma de incorporação os dados secretos são transmitidos em uma conexão codificada tal como de Segurança de Protocolo de Internet (SegPI), ou de camada de soquete seguro (SSL - *Secure Socket Layer*), ou outra forma de encriptação entre o cliente e o servidor.

Conforme ilustrado na figura 1, cada uma das mensagens M1, M2 e M3 tem um campo de identificador secreto 18, mas os identificadores secretos nas mensagens M2 e M3 normalmente não coincidem com os da mensagem M1. Isto é porque os identificadores secretos em uma forma de incorporação são baseados em valores de dados secretos gerados por características

operacionais ou eventos operacionais do dispositivo de cliente, tal como o tempo de envio ou recepção de certas mensagens no dispositivo de cliente ou no servidor, o número de vezes que um certo tipo de mensagem de dados ou pacote de rede foi recebido, e similares. O identificador secreto pode compreender diferentes valores de dados secretos gerados operacionalmente contidos em regiões diferentes do campo de dados secretos, ou pode compreender uma versão transformada de tais valores de dados secretos. É extremamente improvável que tais valores em dispositivos de cliente clonados sejam idênticos aos valores de dados secretos em um dispositivo de cliente real, uma vez que a operação do dispositivo de cliente clonado normalmente não coincide com a operação de um dispositivo de cliente ou de outro dispositivo de cliente clonado. Por exemplo, um primeiro segmento do campo de dados secretos pode conter a primeira potência em um momento de tempo de um dispositivo de cliente em micro-segundos. Depois de um certo período de tempo ou número de eventos, um segundo segmento do campo de dados secretos pode acrescentar à primeira potência uma potência subsequente em um momento de tempo para o dispositivo (por exemplo T1, T2). Embora o servidor não saiba se a segunda potência em um momento de tempo foi adicionada pelo dispositivo de cliente ou por um dispositivo de cliente clonado, é extremamente improvável que a potência no momento de tempo original T1 seja idêntica para ambos os dispositivos, e o segundo e os itens de dados secretos subsequentes acrescentados aos dados secretos trocados entre o cliente e o servidor são projetados para serem únicos entre clientes, e porque os itens de dados secretos adicionais são gerados durante a operação continuada do cliente a probabilidade dos dados secretos serem idênticos é muito baixa.

O servidor recebe mensagens de dispositivos de cliente autênticos e/ou clonados e salva os identificadores secretos mais recentes associados com as credenciais do cliente do usuário autorizado em um módulo de armazenamento de dados secretos de servidor 23. Quando uma mensagem subsequente é recebida, a qual aparentemente vem de um dispositivo associado com as mesmas credenciais do cliente, o servidor compara o identificador secreto com o identificador secreto previamente armazenado para aquele

cliente. Se nenhuma coincidência for encontrada em um ou mais identificadores secretos, é provável que um dos dispositivos que se comunicam com o servidor seja um dispositivo-clone, e o servidor informa a um operador que um clone foi detectado. O
5 operador pode então iniciar procedimentos para determinar qual dispositivo é um dispositivo de cliente válido ou autorizado e qual dispositivo é um clone.

A figura 4 é um diagrama de fluxo ilustrando uma forma de incorporação de um método de uso do sistema das figuras
10 1, 2B e 3 para descobrir a presença de dispositivos de cliente clonados em uma rede. Na etapa 40, um dispositivo de cliente envia uma mensagem ao servidor contendo um identificador secreto no campo de dados secretos 18. A mensagem pode ser no formato ilustrado na figura 2B, por exemplo, ou pode ser qualquer outro
15 tipo de mensagem de comunicação de rede padrão com um identificador secreto compreendendo um ou mais valores de dados secretos inseridos em um campo de dados selecionado na mensagem, ou um identificador que é uma versão transformada de um ou mais valores de dados secretos. O servidor recebe a mensagem e extratos
20 o identificador secreto da mensagem (42), e então compara o identificador secreto com o identificador secreto armazenado correspondendo às credenciais de cliente associadas com o dispositivo de cliente registrado a partir do qual a mensagem parece se originar (etapa 44). O servidor determina se há uma
25 coincidência (etapa 45) baseado na comparação, isto é, determina se há uma coincidência entre qualquer parte de um identificador secreto armazenado e o identificador secreto na mensagem. Se uma coincidência for encontrada, o servidor envia uma resposta de mensagem ao dispositivo de cliente (etapa 48) quando for
30 apropriado, armazena o novo identificador secreto, e o serviço desejado ou transação acontece. Se uma coincidência não for encontrada, isto é não há nenhuma coincidência entre nenhuma parte dos identificadores secretos, o servidor gera um relatório ao operador indicando que um clone em potencial foi detectado (etapa
35 46), e um sinalizador opcional pode ser colocado na memória. Se o identificador secreto é um código de múltiplos dígitos criado pela transformação de valores de dados secretos, uma coincidência

significa que um identificador secreto recebido é idêntico a um identificador secreto armazenado. Se o identificador secreto for um ou mais valores de dados secretos baseados em eventos acontecendo, o identificador secreto recebido pode coincidir
5 somente com parte do identificador secreto previamente armazenado, enquanto ele inclui novos valores de dados secretos acrescentados depois da última mensagem ao servidor. Uma coincidência ainda é encontrada se parte do identificador secreto recebido coincidir com o identificador secreto armazenado, mas uma coincidência não é
10 encontrada se não houver nenhuma coincidência em nenhuma parte do identificador secreto.

O servidor pode continuar as comunicações com o dispositivo que enviou a mensagem quando um clone potencial é detectado, uma vez que ainda não foi determinado se ou não aquele
15 dispositivo é um dispositivo de cliente clonado, isto é, o servidor não tem informação suficiente para determinar qual dos dois dispositivos de cliente se comunicando com o servidor é um clone. Em uma última etapa, o serviço pode ser descontinuado para um dispositivo que é julgado ser um clone, ou para todos os
20 dispositivos, deixando-se que o assinante autorizado contacte o provedor de serviço para arranjar que o seu serviço seja continuado.

Em uma forma de incorporação, os valores de dados secretos nos quais o identificador secreto é baseado pode ser
25 gerado por certos eventos operacionais em um dispositivo de cliente. Alguns exemplos de possíveis valores de dados secretos gerados por eventos operacionais são:

a) Número de vezes em que um cliente executou um certo evento tal como requisitar uma chave ou inicializar uma
30 sessão com um servidor, ou executar uma transação de comércio eletrônico.

b) O número de itens anteriores comprados por um assinante.

c) O número de atualizações de chave de
35 transiente recebidas por um cliente.

d) O momento do tempo da última atualização de *firmware*.

e) O momento do tempo da última requisição de chave para o cliente.

f) O momento do tempo da última mensagem de um tipo particular, ou a contagem do número de vezes em que uma certa
5 mensagem foi recebida, ou o atraso entre a mensagem atual e a mensagem anterior sendo recebida do servidor.

g) O momento do tempo em que um certo tipo de mensagem foi recebida pelo cliente.

h) O momento do tempo em que um certo tipo de
10 mensagem foi recebida do cliente.

i) A contagem do número de vezes em que um certo tipo de mensagem de dados ou pacote de rede foi recebido com exemplos incluindo MCE (Mensagens de Controle de Entitulação) de vídeo, contagem de diferentes valores de MPEG2 PID, contagem de
15 pacotes em um número de porta de TCP PI particular, etc.

j) O atraso de tempo entre uma mensagem de requisição sendo enviada à rede e a resposta que é recebida de volta do servidor.

k) O último momento de tempo em que uma união de
20 multidifusão foi executada, ou o valor da última união de multidifusão.

l) o endereço de PI provido pelo servidor de Protocolo de Configuração de Hospedeiro Dinâmico (PCHD) quando um PCHD é usado no sistema.

25 m) O tempo remanescente em um arrendamento de PCHD quando um PCHD é usado no sistema.

n) Os valores obtidos de outros dispositivos de rede tais como os parâmetros de faixa para um modem a cabo ou a força do sinal da rede depois de 3 dias de uso com um novo
30 cliente.

o) A troca de dados ou uma nova mensagem sendo gerada depois de um certo período de tempo, por exemplo quando o dispositivo de cliente recebe um valor de dados secretos do servidor, que indica ao dispositivo de cliente em quantos minutos
35 o dispositivo de cliente deve contactar o servidor.

p) O valor de um parâmetro de dados de cliente após um número de eventos, tal como o número do canal de TV quando 57 mudanças de canal ocorreram.

q) Um novo valor de dados secretos derivado de um valor de dados secreto previamente usado processado com uma função que cria o novo valor de dados secreto.

r) Um valor de dados secreto gerado a partir de dados dentro de um *chip* no dispositivo de cliente, ou um valor de dados secreto gerado a partir dos dados processados ou escalados de um *chip* ou placa ou cartão conectável de *hardware* ou memória segura no dispositivo de cliente.

s) Um valor de dados secretos tal como um símbolo ou chave recebidos do servidor, que o dispositivo de cliente retém e usa como parte de um identificador secreto contendo um ou mais valores ou itens de dados secretos em mensagens subseqüentes com o servidor. Os dados secretos recebidos do servidor podem ser transformados pelo dispositivo de cliente e a versão transformada pode ser devolvida ao servidor como um identificador secreto em mensagens subseqüentes. Isto permite que o servidor passe símbolos ou chaves ao cliente em mensagens normais entre o cliente e o servidor como parte das mensagens normais de sistema. O símbolo provido pelo servidor usado para o identificador secreto de cliente pode ser enviado em uma mensagem separada, mas a mensagem preferida passa o valor de dados secretos a partir do servidor em uma mensagem normal.

t) O momento do dia em que o 12.000º pacote de rede foi recebido.

Alguns dos valores listados acima podem adicionalmente ou alternativamente ser usados como ativadores de evento ou contadores de eventos que ativam a atualização ou modificação de identificadores secretos contidos em um protocolo de mensagens entre um dispositivo de cliente e um servidor. Por exemplo, um evento operacional pode ativar um contador que conta eventos operacionais subseqüentes, tal como o número de mudanças de canal em um dispositivo de cliente, por exemplo, e registra um valor de dados secretos sobre quando o usuário trocou canais um número pré-determinado de vezes. O valor de dados secreto pode ser

o momento do dia em que a pré-determinada contagem foi alcançada, ou o tempo gasto antes da contagem pré-determinada ser alcançada. Outros tipos de eventos operacionais podem ser contados da mesma maneira para prover um ativador de evento, tal como o número de mensagens de um certo tipo enviadas ou recebidas por um dispositivo de cliente, o número de itens comprados, ou similares, ou o próprio número de eventos pode ser usado diretamente como valor de dados secretos. Outros possíveis ativadores de eventos podem ser o momento do tempo em que um evento operacional acontece, tal como uma atualização de *firmware*. Tais ativadores de evento podem ser usados para trocar um prévio conjunto de valores de dados secretos por um novo conjunto de valores de dados secretos baseado em eventos operacionais diferentes, com os novos valores de dados secretos sendo usados então para criar o identificador secreto. Isto torna muito mais difícil que os piratas (*hackers*) determinem quais eventos operacionais particulares são usados para gerar o identificador secreto.

Os dados secretos 18 podem ser construídos em uma tabela. Uma forma de incorporação de uma possível tabela de dados secretos é mostrada na Tabela 1 abaixo. Na tabela mostrada abaixo a tabela de dados secretos é construída usando dois itens ou valores de dados secretos. Um item de dados secreto é o momento do dia (MDD) em que a mais recente mensagem de requisição de chave de radiodifusão (CRad) foi feita e o outro é o número de atualizações de chave de transiente obtido por um dispositivo de cliente tal como uma caixa de interface (STB) ou outro dispositivo de cliente. Outros itens de dados secretos baseado em características operacionais podem ser usados em formas de incorporação alternativas, e mais de dois itens de dados secretos podem ser usados para segurança adicional. Inicialmente ambos os valores na Tabela 1 são 0, e o identificador secreto inicial pode ser 0, 0. A Tabela 1 abaixo é apenas um exemplo de dois valores de dados que podem estar junto em uma versão de um lançamento do *software* de um cliente. É previsto que outros valores de dados secretos possam ser usados para criar um identificador secreto e que diferentes valores de dados podem ser usados entre diferentes versões de *software*. Por exemplo, neste exemplo o número de atualizações de

chave de transiente está sendo usado, mas em outra versão do software o momento do dia (MDD) da última atualização de chave de transiente poderia ser usado, ou o número de segundos entre as primeira e segunda atualizações de chave de transiente poderia ser usado.

TABELA 1 - Tabela de Dados Secretos

Dados Secretos	Descrição
MDD da primeira requisição de CRad	O Momento Do Dia em que a primeira ou enésima requisição de Chave de Radiodifusão (CRad) foi feita pelo dispositivo de cliente. Inicialmente isto é configurado para 0.
Número de atualizações de chave de transiente	O número de vezes em que o dispositivo de cliente teve sua chave de transiente atualizada. Inicialmente isto é configurado para 0.

As figuras 5A e 5B ilustram um diagrama de fluxo das etapas do método em um exemplo de uma forma de incorporação para detectar dispositivos-clone usando dados secretos como na Tabela 1 acima. A Tabela 2 abaixo ilustra um possível exemplo de valores de dados secretos armazenados tanto no servidor como no dispositivo de cliente ou dispositivo de cliente clonado em várias etapas nas figuras 5A e 5B, e as figuras 6A a 6F ilustram mensagens geradas em várias fases no exemplo das figuras 5A e 5B. Na Tabela 2 e na figura 5, o termo "dispositivo de cliente real" é usado para designar o dispositivo de cliente original ou autêntico associado com as credenciais de dispositivo de cliente registradas no servidor, enquanto o termo "dispositivo de cliente clonado" se destina a um dispositivo de cliente que é uma cópia exata do dispositivo de cliente real com as mesmas credenciais. Na etapa 100 da figura 5A, um dispositivo de cliente real ou autêntico é instalado e registrado como associado com um assinante para os serviços providos pelo servidor 10, que salva as credenciais do dispositivo de cliente de assinante em um banco de dados 20. No primeiro acionamento do dispositivo de cliente 14 (etapa 101), o identificador secreto é inicializado (etapa 102) para um valor inicial conhecido tanto no banco de dados do servidor como no banco de dados do dispositivo de cliente. O identificador secreto

neste caso compreende um conjunto de valores de dados secretos conforme indicado na Tabela 2 abaixo. Neste exemplo, pelo menos um dos valores de dados secretos usado no identificador secreto é o momento do dia (MDD) no qual uma requisição de chave de radiodifusão (CRad) foi feita pelo dispositivo de cliente, embora quaisquer outros valores de dados secreto possam ser usados em lugar do MDD da requisição de CRad ou em adição ao MDD em outras formas de incorporação.

Os valores de dados secreto iniciais conforme armazenados no banco de dados do servidor 20 antes que qualquer requisição de CRad tenha sido recebida são MDD Reconhecido (Reco) = 0, MDD Não-Reconhecido (NReco) = 0, isto é, o identificador ou dados secretos para este cliente no servidor são 0, 0, enquanto o valor de dados secreto inicial armazenado no dispositivo de cliente quando é acionado pela primeira vez é MDD = 0. Como esta é a primeira aplicação de acionamento depois que o dispositivo de cliente foi instalado, o ativador de evento de MDD para a requisição de chave de radiodifusão é zero, porque o dispositivo de cliente ainda não requisitou chaves de radiodifusão. Qualquer um ou todos os dados secretos podem ser configurados em um estado inicial tal como zero no primeiro acionamento de um dispositivo de cliente e/ou no servidor antes da recepção de uma primeira mensagem vinda de um dispositivo de cliente. Em formas de incorporação alternativas, um ou mais valores de dados secretos não-zero podem ser gerados durante o processo de inscrição quando o dispositivo de cliente de um assinante é registrado no servidor, e usados para criar um identificador secreto inicial, ou incluídos em um identificador secreto além de um ou mais valores de dados secretos que são inicialmente configurados em zero.

Na Tabela 2, o valor não reconhecido (NReco) de um item de dados secreto armazenado no servidor é o último valor emitido para um dispositivo de cliente (real ou clonado) por um servidor que ainda não foi reconhecido em uma mensagem vinda do dispositivo de cliente. O valor de NReco é movido para a coluna de Reconhecido (Reco) do valor armazenado no servidor quando o cliente retorna o valor de NReco ou um valor derivado pelo dispositivo de cliente a partir do valor de NReco. O cliente pode

retornar o valor de NReco na próxima mensagem ao servidor em uma forma de incorporação, como ilustrado na Tabela 2 e nas figuras 5 e 6. Em uma forma de incorporação alternativa (não ilustrada), o dispositivo de cliente envia uma mensagem de reconhecimento específica ao servidor após a recepção do novo valor de NReco, confirmando que o valor de NReco foi armazenado com sucesso no banco de dados do dispositivo de cliente. Neste momento, o valor de NReco substitui o valor de Reco no servidor. Porém, esta alternativa é mais susceptível a *hackers* (piratas), que obtém o valor de dados secreto. O método ilustrado nas figuras 5A e 5B nos quais o único reconhecimento do valor de NReco acontece quando a próxima mensagem de um tipo designado é enviada ao servidor, é mais secreto.

Depois da inicialização, o dispositivo de cliente envia uma requisição por chaves de radiodifusão (requisição de CRad) para o servidor na etapa 104. Em uma forma de incorporação, esta requisição contém um identificador secreto ou dados de segurança secretos 18. O identificador secreto na mensagem de CRad neste caso é como se segue:

MDD da última requisição de CRad = 0
 Atualizações de chave de transiente = 0
 Em outras palavras, o identificador secreto na requisição de CRad é 0, 0, e o formato desta mensagem M1 é ilustrado na figura 6A.

O servidor recebe a requisição de CRad (etapa 105), e extrai os valores de dados secretos no identificador secreto a partir da requisição, então confere estes valores contra os valores correspondentes armazenados no servidor. Esta comparação é descrita abaixo para o valor de dados secretos de MDD de CRad somente em uma série de mensagens, mas uma comparação semelhante é executada para outros valores de dados secretos em um identificador secreto, tal como um valor baseado em atualizações de chave de transiente. Como esta é a primeira mensagem de qualquer dispositivo de cliente usando estas credenciais de cliente, os dados de MDD de CRad coincidem (etapa 108), e o servidor retorna as CRads ao dispositivo de cliente (etapa 110) com um valor de MDD T1 determinado pelo servidor, isto é, o

momento do dia da recepção no servidor da primeira requisição de CRad deste cliente. Uma forma de incorporação do formato da mensagem de resposta de CRad R1 é ilustrada na figura 6B na qual o novo valor de MDD T1 é provido em um campo de mensagem depois do ID e NS de mensagem. Em uma forma de incorporação alternativa, o valor de MDD para a mensagem pode ser lido localmente pelo dispositivo de cliente, em vez de ser recebido na mensagem vinda do servidor. O valor de MDD recebido do servidor pode ser substituído com qualquer tipo de valor de dados ou símbolo enviado do servidor, em outras formas de incorporação alternativas.

No exemplo provido na Tabela 2 abaixo, o valor de MDD T1 é 8437, e é acrescentado ao banco de dados do servidor como um MDD de NReco na etapa 114 uma vez que nenhum reconhecimento da recepção deste valor ainda não foi recebido do dispositivo de cliente. Como visto acima, o dispositivo de cliente pode ser programado para enviar um reconhecimento de recepção do valor de MDD T1 em uma forma de incorporação alternativa, mas nesta forma de incorporação nenhum reconhecimento é enviado até a próxima mensagem de CRad, e assim o valor de MDD T1 permanece um valor de NReco até e a menos que seja reconhecido em uma mensagem de CRad subsequente, que é uma opção mais secreta. Neste momento, os valores de MDD no identificador de cliente salvos no servidor são MDD de Reco = 0, MDD de NReco = T1 ou 8437 neste exemplo.

TABELA 2 - Exemplo de valores de dados secretos em várias etapas na figura 5

Etapas	Ações do Servidor	BD do Servidor	Valores de Dados Secretos no cliente	Ações do Dispositivo de cliente/clone
101, 102	Os valores de dados secretos iniciais para um dispositivo de cliente são inicializados para um valor inicial conhecido.	MDD de Reco=0 MDD de NReco=0	MDD = 0	Todos os dados secretos em um estado inicial (0,0).

Etapa	Ações do Servidor	BD do Servidor	Valores de Dados Secretos no cliente	Ações do Dispositivo de cliente/clone
112, 114	O servidor retorna CRads com um valor de Momento Do Dia (MDD) determinado pelo servidor. O servidor adiciona o(s) último(s) valor(es) de dados secretos ao BD do servidor como valor(es) não-reconhecido(s). O BD contém o último bom valor conhecido (0 neste exemplo) mais o último valor não-reconhecido (MDD atual = 8437).	MDD de Reco=0 MDD de NReco=8437 Note-se que 8437 é um novo MDD provido pelo servidor ao cliente.		
115, 116			MDD agora igual a 8437.	Dispositivo de cliente real salva MDD da última CRad passada do servidor na mensagem de distribuição de CRad na memória não-volátil.
122		MDD de Reco=0 MDD de NReco=8437	MDD = 0	Os dados secretos de dispositivo de cliente clonado na requisição de CRad são como se segue: MDD da última requisição de CRad=0 Atualização de chave de transiente=0

Etapa	Ações do Servidor	BD do Servidor	Valores de Dados Secretos no cliente	Ações do Dispositivo de cliente/clone
126, 130	O servidor retorna CRads com um novo valor de Momento Do Dia (MDD) determinado pelo servidor. O servidor adiciona o(s) último(s) valor(es) de dados secretos ao BD do servidor como valor(es) não-reconhecido(s). O BD contém o último bom valor conhecido (0 neste exemplo) mais o último valor não-reconhecido (MDD atual).	MDD de Reco=0 MDD de NReco=9902 Note-se que 9902 é um novo MDD provido pelo servidor ao cliente, eliminando o valor não-reconhecido 8437 enviado a outras STBs requisitando chaves antes da STB clonada.		
132			MDD no clone é 9902.	O dispositivo de cliente clonado salva o MDD recebido do servidor na mensagem de distribuição de CRad.
134		MDD de Reco=0 MDD de NReco=9902	MDD no dispositivo de cliente real é 8437	Cliente real envia mensagem de CRAD renovada ao servidor com o MDD de Reco da última requisição de CRad=8437, e Atualização de Chave de Transiente=0.
135	O servidor recebe requisição de CRad e confere MDD no BD contra o MDD na requisição.	MDD de Reco=0 MDD de NReco=9902	MDD de Reco=8437	

Etapa	Ações do Servidor	BD do Servidor	Valores de Dados Secretos no cliente	Ações do Dispositivo de cliente/clone
140, 142	O servidor atualiza o MDD de NReco para 11305 e envia CRads e MDD à STB	MDD de Reco=0 MDD NReco=11305	MDD no dispositivo de cliente real é 11305	

Na etapa 115, o dispositivo de cliente real recebe as chaves de radiodifusão na resposta do servidor, junto com o novo valor de MDD T1 (neste exemplo 8437). O dispositivo de cliente então armazena o novo valor de MDD (etapa 116), e decifra os dados encriptados tais como os dados de radiodifusão vindos do servidor usando as chaves de radiodifusão (etapa 118). No exemplo ilustrado, um dispositivo de cliente clonados é acionado (120) algum tempo depois que as primeiras chaves de radiodifusão são recebidas pelo dispositivo de cliente real e antes o dispositivo de cliente real envia uma requisição de chave de radiodifusão subsequente para o servidor. Esta sequência de eventos não acontece em todos os casos, e é somente um exemplo possível de uma sequência de comunicações de dispositivo de cliente real e clonado com o servidor. O dispositivo de cliente clonado envia uma requisição de chave de radiodifusão ao servidor (122) contendo um identificador secreto compreendendo valores de dados secretos iniciais 0, 0, e um possível formato desta mensagem M2 é ilustrado na figura 6C. A primeira mensagem de qualquer dispositivo de cliente clonado nesta forma de incorporação contém o mesmo identificador secreto como a primeira mensagem do dispositivo de cliente autêntico ou real, isto é 0, 0. Se esta mensagem for recebida pelo servidor antes que o dispositivo de cliente real tenha reconhecido um novo valor de MDD do servidor, o servidor ainda não tem nenhum modo de saber que existe um dispositivo de cliente clonado. Se ela for recebida depois que um novo valor de MDD foi reconhecido pelo mesmo dispositivo de cliente que inicialmente requisitou CRads, o servidor sabe que há dois dispositivos de cliente no sistema usando credenciais idênticas, e gera um relatório de detecção de clone conforme a figura 4.

No exemplo das figuras 5A e 5B, um dispositivo de cliente clonado envia a primeira requisição de CRad ao servidor antes do dispositivo de cliente real acusar o recebimento de um novo valor de MDD vindo do servidor. Após a recepção da requisição de CRad, o servidor extrai os valores de dados secretos 0, 0 e compara estes valores com os valores de dados secretos armazenados para o dispositivo de cliente real tendo as mesmas credenciais (etapa 124). Neste ponto, uma coincidência de dados secretos é encontrada (etapa 125), isto é, os dados secreto recebidos estão corretos, uma vez que nenhum reconhecimento específico de recebimento do MDD de NReco T1 (por exemplo 8437) ainda não foi recebido do dispositivo de cliente. Neste exemplo particular, o servidor não sabe se a mensagem contendo o MDD nunca foi recebida pelo dispositivo de cliente por alguma razão, tal como falha de rede ou desligamento do dispositivo de cliente, e então não assume que algum dispositivo clonado está presente. O banco de dados do servidor contém o último bom valor conhecido do MDD (neste caso 0) mais o último calor T1 de MDD não reconhecido. Considerando que o valor reconhecido é uma coincidência, o servidor envia as chaves de radiodifusão ao dispositivo de cliente clonado com um novo valor de MDD T2 (etapa 126) em uma mensagem de resposta que pode ter o formato ilustrado na figura 6D, em uma forma de incorporação. No exemplo particular provido na Tabela 2 acima, o valor de T2 é 9902. Ao mesmo tempo, o MDD de NReco no servidor é mudado para T2 (ou 9902 neste exemplo) na etapa 30, como ilustrado na figura 5B, eliminando o MDD de NReco T1 previamente armazenado (ou 8437 no exemplo da Tabela 2).

O cliente clonados recebe a mensagem de CRad e o novo valor de MDD T2 na mensagem do servidor e salva o novo valor de MDD T2 (etapa 132), e procede em decifrar os dados tais como os dados de radiodifusão recebidos do servidor (etapa 133). No exemplo ilustrado na figura 5B, a próxima comunicação com o servidor depois da etapa 132 é uma mensagem enviada do dispositivo de cliente real requisitando chaves de radiodifusão (Requisição de CRad) uma vez que o dispositivo de cliente real precisa renovar suas CRads (etapa 134). Esta mensagem pode ter o formato ilustrado na figura 6E e contém um identificador secreto compreendendo os

valores de dados secretos atualmente armazenados no dispositivo de cliente real, especificamente o MDD da última requisição de CRad deste dispositivo de cliente (T1 ou 8437) e o número de atualização de chave de transiente (0 neste exemplo). Na etapa 5 135, o servidor recebe a nova mensagem de CRad do dispositivo de cliente real e compara os valores de MDD de Reco e NReco correntemente armazenados (especificamente 0 e T2 ou 9902) com o valor de MDD T1 ou 8437 recebido no identificador secreto do dispositivo de cliente. Considerando que o valor que T1 recebido 10 do dispositivo de cliente não é igual nem ao valor de Reco 0 armazenado no servidor, nem ao valor de NReco T2 armazenado no servidor (etapa 136), o servidor informa a detecção de clone ao operador de sistema para uma ação posterior (etapa 138). Outro processamento do lado do servidor pode ser aplicado neste momento 15 para detectar clones. O servidor não nega o serviço uma vez que ele não pode determinar qual dos dois dispositivos de cliente enviando mensagens é o dispositivo de cliente real ou autêntico, e então envia CRads e um novo valor de MDD T3 (11305 no exemplo da Tabela 2 acima) para o dispositivo de cliente real (etapa 140) em 20 uma mensagem de resposta que pode ter o formato ilustrado na figura 6F. O servidor então armazena o novo valor de MDD T3 como um valor de NReco no banco de dados do servidor (etapa 142), e o dispositivo de cliente real também armazena o novo MDD T3.

O método das figuras 5A e 5B ilustra um possível 25 método e sequência de eventos nos quais um dispositivo de cliente clonado envia uma mensagem a um servidor depois que o dispositivo de cliente real recebeu sua primeira CRad do servidor mas antes o dispositivo de cliente real requisita CRads renovadas ao servidor. Tais eventos podem acontecer em sequências diferentes dependendo 30 do uso dos dispositivos de cliente verdadeiro e clonado, e mais de dois dispositivos de cliente com as mesmas credenciais podem enviar mensagens a um servidor durante o mesmo período de tempo. Os dispositivos de cliente clonados podem enviar mensagens ao servidor a qualquer momento e em qualquer ordem em relação a 35 mensagens semelhantes enviadas por um dispositivo de cliente real. Sem considerar a ordem, o servidor pode determinar a presença de um dispositivo de cliente clonado porque o valores de dados

secrets em mensagens tanto do dispositivo de cliente real ou de um ou mais dispositivos de cliente clonados não coincidem com um ou mais valores atualmente armazenados no servidor. Por exemplo, referindo-se à figura 5A e à etapa 122 da Tabela 2, se o

5 dispositivo de cliente real envia um a requisição de CRad subsequente ao servidor nesta fase, antes de qualquer mensagem ser enviada por um dispositivo de cliente clonado, então os valores de dados secretos na requisição de CRad são T1, 0 ou 8437, 0 no exemplo específico da Tabela 2. O servidor que recebe esta

10 mensagem nota a coincidência entre o valor de MDD do dispositivo de cliente e o MDD de NReco salvo em seu banco de dados, e muda o MDD de Reco de 0 para T1. Um novo MDD de NReco T2 é então enviado na resposta ao dispositivo de cliente. Um dispositivo de cliente clonado comunicando-se subsequentemente com o servidor envia um

15 MDD = 0, já que é a primeira comunicação daquele dispositivo com o servidor. Este MDD não coincide com o MDD de Reco (T1) ou com o MDD de NReco (T2) armazenados no servidor, e um relatório de detecção de clone é gerado pelo servidor. Uma falha de coincidência semelhante acontece em algum ponto em qualquer

20 sequência de mensagens quando mais de um dispositivo de cliente usando as mesmas credenciais está se comunicando com um servidor, sem considerar a ordem das comunicações entre um servidor e um dispositivo de cliente real e dispositivos de cliente clonados.

Na forma de incorporação das figuras 5 e 6, e no

25 exemplo específico desta forma de incorporação esboçado na Tabela 2 acima, o identificador secreto em cada mensagem compreende dois ou mais valores de dados secretos. Porém, o identificador secreto pode incluir um código gerado baseado em tais valores de dados secretos, por exemplo transformando os valores usando uma função

30 de adequação de dados (*hash*) ou similar. A mensagem contendo o identificador secreto é uma requisição de chave de radiodifusão na forma de incorporação acima, e o dispositivo de cliente recebe uma radiodifusão do servidor. O dispositivo de cliente neste caso é um reproduutor de mídia tal como uma caixa de interface de televisão,

35 um computador pessoal, ou qualquer outro dispositivo de cliente capaz de reproduzir radiodifusão, tal como radiodifusão de televisão. O servidor pode ser um que distribua chaves de

decriptação de canal de televisão de radiodifusão para os clientes. Porém, outros tipos de dispositivo de cliente e provedores de serviço podem usar as mesmas técnicas de dados secretos em tipos diferentes de mensagens. Como visto acima, as técnicas de dados secretos das formas de incorporação acima podem ser aplicadas a qualquer tipo de provedor de serviço de rede e a qualquer tipo de dispositivo de cliente conectado a servidores do provedor de serviço, tais como computadores pessoais, telefones celulares, assistentes digitais pessoais (ADPs), equipamentos de vídeo (TIVO, DVD, CD, etc.), e qualquer outro tipo de dispositivo de cliente, e para qualquer tipo de serviço tal como transações bancárias *on-line*, comércio eletrônico, inscrição de dados, sistemas de comunicações de mensagens, etc. Na forma de incorporação acima, as chaves de decriptação de canal de televisão de radiodifusão (CRads) são as chaves necessárias para decifrar canais de TV de radiodifusão encriptados, como é tipicamente usado para canais de televisão *premium* ("prêmio"), tal como *Home Box Office* (HBO) ou o Canal de Filmes (*Movie Channel*). Canais de televisão "prêmio" são canais opcionais que um assinante de TV de protocolo de internet (PI) ou de TV a cabo pode escolher comprar. As técnicas aqui descritas também são aplicáveis a quaisquer técnicas de encriptação onde as chaves são distribuídas a dispositivos de cliente para permitir o acesso a vários tipos de serviços de rede, ou podem ser usadas em diferentes tipos de mensagens entre um servidor e um dispositivo de cliente além de, ou em vez de, mensagens de requisição de chaves de decriptação.

Porque há a possibilidade de que um dispositivo de cliente real não receba uma mensagem de um servidor devido a uma falha de rede ou devido ao dispositivo de cliente ser desligado antes que a mensagem de resposta seja recebida, a forma de incorporação das figuras 5A e 5B pode incluir um processamento do lado do servidor para reduzir o número de falsos alertas de detecção de clone gerados, por meio do que um alerta de detecção de clone é uma indicação de que um cliente foi detectado com credenciais de cliente idênticas às de outro cliente. Em uma forma de incorporação alternativa, como mencionado acima, um reconhecimento de cliente interpretado é enviado do dispositivo de

cliente a cada vez que um ítem de dados secretos usado em um identificador secreto é atualizado, e o servidor coordena o ítem de dados secreto esperado no banco de dados do servidor baseado no reconhecimento do cliente de que um ítem de dados secretos provido pelo servidor foi recebido e armazenado com sucesso pelo cliente. O uso de uma mensagem de reconhecimento direta entre o cliente e o servidor indicando que um símbolo de dados secretos do servidor foi armazenado pelo cliente, ou que o ítem de dados secretos do cliente foi reconhecido pelo servidor, pode melhorar a detecção de clones mas pode criar mensagens adicionais que são processadas pelo servidor e podem ser interceptadas por *hackers*.

Em uma forma de incorporação, o servidor envia ítems ou símbolos de dados secretos únicos a um dispositivo de cliente para uso em mensagens subseqüentes. Exemplos de ítems ou valores de dados que o servidor pode enviar ao dispositivo de cliente incluem valores de dados temporários periodicamente modificados pelo servidor quando o cliente e o servidor se comunicam, chaves temporárias enviadas do cliente ao servidor, e similares. Em uma forma de incorporação, o servidor envia chaves de encriptação/decriptação temporárias ou transientes a um cliente e as chaves de transiente se tornam parte do anel de chaves usado na encriptação de mensagens entre o cliente e o servidor. O uso de chaves de transiente impede que os clientes clonados se comuniquem com o servidor porque somente um cliente contém as chaves apropriadas para conseguir as comunicações encriptadas entre um cliente e um servidor. As chaves de transiente podem ser enviadas em um canal de comunicações encriptadas à base de sessão tal como provido por SSL ou provido por trocas de chave do tipo Diffie Hellman de modo que os pacotes de rede contendo as chaves de transiente atualizadas providas pelo servidor não podem ser decifrados por dispositivos clonados que obtêm as mesmas mensagens de atualização de chave de transiente. Tal encriptação baseada em sessão pode ser usada para qualquer tipo de comunicação. Em uma forma de incorporação, o servidor envia um símbolo ou símbolos ao dispositivo de cliente, que são armazenados pelo dispositivo de cliente e usados em mensagens subseqüentes de cliente-para-

servidor. O servidor pode prover um símbolo único em momentos aleatórios ou a intervalos fixos para um dispositivo de cliente.

No exemplo da Tabela 2, são mostrados dois valores de dados secretos. Porém, um, dois ou mais valores de dados secretos podem ser usados com valores que são providos exclusivamente pelo servidor e/ou valores que são exclusivamente determinados pelo cliente baseado na operação do dispositivo de cliente. Em uma forma de incorporação, o módulo de dados secretos 29 no dispositivo de cliente pode incluir uma memória não-volátil, e partes de, ou todos os, dados secretos podem ser armazenados localmente na memória não-volátil (disco rígido, memória *Flash*, ou similares) no dispositivo de cliente. A ordem de acionamento de dispositivos de cliente reais e clonados ou a ordem na qual eles se conectam a uma rede, ou a ordem em que eles fazem uma primeira conexão com o servidor, não é importante e as técnicas acima descritas não exigem que os dispositivos de cliente sejam acionados em qualquer ordem. Assim, o primeiro dispositivo de cliente acionado nas figuras 5A e 5B pode ser um dispositivo de cliente clonado em lugar de um dispositivo de cliente real, e dispositivos de cliente reais e clonados podem se comunicar com o servidor em qualquer ordem e em qualquer momento. Sem considerar a ordem das mensagens, esta forma de incorporação permite que o servidor determine quando houver mais de um dispositivo de cliente usando as mesmas credenciais de cliente, quando uma mensagem for recebida na qual o valor de dados secretos não coincide com os valores de dados secretos no servidor, indicando que um dispositivo de cliente real foi clonado.

As figuras 5A e 5B ilustram a detecção de clone secreto usando um único item de dados secreto que é enviado do servidor a um dispositivo de cliente na forma do Momento do Dia (MDD) da última requisição de um dispositivo de cliente. Em uma forma de incorporação alternativa, podem ser usados um ou mais ativadores secretos. Um ativador secreto é um ativador que ocorre depois que um número de eventos acontecem e que responde modificando os dados secretos usados para criar o identificador secreto, ou provendo um novo pedaço de dados secretos que pode ser rastreado pelo servidor. Há numerosos ativadores secretos

possíveis na operação normal de um dispositivo de cliente, e os ativadores secretos ou eventos podem ser baseados em múltiplas categorias de eventos tal como tempo (número total de horas em que o dispositivo de cliente ficou ativo, número aleatório de horas depois que o dispositivo de cliente foi instalado ou atualizado, ou similares), mensagens (número total de mensagens de controle de entitulação de vídeo ou MCEs recebidas, total de mudanças de canal), ou processamento de dados internos (por exemplo MDD quando o 100.000º pacote de vídeo foi decifrado). Outros exemplos de um 5 ativador secreto incluem um ativador que ocorre quando um dispositivo de cliente tal como uma caixa de interface (STB) trocou de canais 100 ou 200 vezes, por exemplo, ou um ativador que acontece quando um certo número de eventos de cliente acontecem e o ativador salva o momento do dia do cliente (ou outro parâmetro) 10 quando o ativador ocorre. Outro exemplo é o valor atual do 15.000º pacote de MCE recebidas, ou o Momento Do Dia (MDD) quando o 15.000º pacote de MCE foi recebido ou uma adequação de dados (*hash*) dos dois valores de dados. Eventos que ativam a criação de um valor de dados secreto acontecem a taxas diferentes em dois 15 dispositivos de cliente com credenciais idênticas (dispositivos de cliente autênticos/reaís e clonados), de maneira que o dispositivo de cliente autêntico ou real e os dispositivos de cliente clonados têm dados secretos diferentes, e então identificadores secretos diferentes. Os identificadores secretos são usados no lado do 20 servidor para detectar múltiplos clientes presentes em uma rede. 25

Em uma forma de incorporação, as bibliotecas de cliente de valores secretos salvos são periodicamente modificadas para salvar novos ou diferentes valores de dados secretos que por sua vez são usados para gerar um identificador secreto. Deste 30 modo, os piratas (*hackers*) que podem ter obtido uma biblioteca de cliente não sabem quando um novo evento que cria um valor de dados secreto usado em um identificador secreto poderá acontecer depois que uma biblioteca de cliente foi atualizada. Os *hackers* precisam deixar todos os dispositivos de cliente clonados fora da rede para 35 evitar detecção depois de uma atualização de *software* da biblioteca de cliente, para tentar determinar quais ativadores secretos são programados na biblioteca de cliente, quando os

ativadores ocorrem, e quais dados secreto são armazenados na biblioteca de cliente em resposta a um ativador. Tais atualizações podem ser geradas por um servidor e podem usar capacidades de processamento seguro contidas dentro do dispositivo de cliente. O método de descarregamento de dados de *firmware* de cliente para atualizar a biblioteca de cliente pode usar imagens de código digitalmente assinadas para permitir que o cliente autentique o descarregamento de dados. O *software* da "extremidade final" pode ter funções de interface de programação de aplicação (IPA) ou uma interface de carrossel de dados para descarregar dados de *software* de cliente.

Em uma forma de incorporação, os identificadores secretos contêm dados que podem ser estáticos para várias requisições e então os dados secretos usados para gerar o identificador secreto mudam, baseado em um ativador secreto, ou o identificador secreto para cada mensagem de um certo tipo muda, tal como o Momento Do Dia ou MDD para a requisição da mensagem anterior. Os dados secretos usados em um identificador secreto podem se originar dentro do dispositivo de cliente, ou serem enviados do servidor como parte das mensagens, ou pode ser uma combinação de dados de cliente/servidor. O identificador secreto pode incluir dados que são processados pelo cliente ou servidor, tal como aplicar valores de dados secretos atuais a uma transformação matemática ou adequação de dados (*hash*) criptográfica.

Em uma forma de incorporação, os valores de dados secretos usados em um identificador secreto também podem mudar baseado no servidor respondendo a uma requisição em um dentre vários modos diferentes. Em um exemplo, as primeiras 10 requisições de chave de radiodifusão recebem um valor de dados secretos e as requisições subseqüentes depois da 10^a recebem uma resposta diferente na qual os dados secreto são modificados ou misturados, ou ambos. As mudanças podem acontecer no lado do cliente ou do servidor, ou em ambos. O identificador secreto é contido em um pedaço ou campo da mensagem como parte de uma mensagem normal processada durante o processamento normal do sistema e o pedaço da mensagem pode variar entre duas diferentes

liberações de código do software de cliente. Além disso, o pedaço da mensagem pode ter dados arbitrários sem sentido aplicados como um branqueador de dados. Em uma forma de incorporação, o pedaço de dados tem de três a cinco valores de dados secretos e os valores de dados secretos mudam baseado em diferentes eventos ou ativadores que ocorrem em momentos diferentes.

Na forma de incorporação descrita acima com relação às figuras 5 e 6, um identificador secreto baseado no momento do dia de uma mensagem é provido em mensagens de requisição de chave de radiodifusão ou similares. A Tabela 3 abaixo ilustra um exemplo de um identificador secreto transformado criado em dispositivos de cliente compreendendo telefones móveis.

TABELA 3 - Identificadores secretos de telefone móvel

	Telefone Real			Clone 1			Clone 2		
ID Móvel (NAE)	100-4452			100-4452			100-4452		
Entrada de Chamada	#	MDD	Dur.	#	MDD	Dur.	#	MDD	Dur.
	N1	8:22	1:06	N3	23:45	7:45	N5	16:41	3:16
	N2	9:11	0:23	N4	1:02	3:36	N6	21:42	10:44
Identificador Secreto	391740			457492			112208		

Na Tabela 3, um telefone é real e os outros dois são clones, e cada telefone cria um identificador secreto baseado na operação do telefone. No exemplo acima somente as primeiras duas entradas de chamada são usadas para gerar um único identificador secreto (ID). A entrada de chamada de cada telefone é processada com uma função do tipo de adequação de dados (*hashing*) criptográfica que gera um único ID secreto para cada telefone, resultando em um identificador que é único para cada telefone mesmo para telefones perfeitamente clonados. Porque os telefones foram clonados na fabricação e cada telefone é usado de maneira ligeiramente diferente com o passar do tempo, os identificadores secretos são extremamente difíceis de duplicar, mesmo se os proprietários dos telefones tentarem criar entradas de chamada idênticas para gerar identificadores secretos idênticos. Isto é porque seria necessário obter eventos em micro-segundos idênticos para criar entradas de chamada perfeitamente idênticas, o que pode ser impossível em dispositivos do mundo real.

Os identificadores secretos entre cliente e servidor podem ser encriptados para segurança adicional, com as chaves de encriptação sendo únicas entre clientes, mas os identificadores secretos podem ser valores de dados secretos não-encriptados em outras formas de incorporação. Em algumas formas de incorporação, a segurança sem chave entre um cliente e o servidor pode ser envolvida, usando apenas os valores de dados secretos ou identificadores secretos baseados em tais valores para identificar dispositivos de cliente. Porém, a segurança é aumentada quando as comunicações de cliente/servidor são encriptadas. Dados secretos ou identificadores secretos podem ser usados de muitas maneiras para identificar operacionalmente um cliente sem a necessidade de um par de chaves de encriptação. Na realidade, o esquema de dados secretos descrito acima pode ser usado em todas as transações de mensagens sem mensagens específicas de segurança sendo requeridas em um sistema. Isto significa que as técnicas de dados secretos aqui descritas podem ser usadas para aumentar a autenticação de clientes com e sem credenciais de segurança tais como certificados X.509, chaves de encriptação, e chaves específicas de segurança semelhantes. Em uma forma de incorporação, todas as comunicações entre um cliente e um servidor ou entre dois dispositivos de computador são melhoradas pelas técnicas aqui descritas em situações onde uma chave específica de encriptação não é requerida. Formas de incorporação podem aplicar todos os tipos de *software* e *firmware* que atuam em um sistema incluindo *softwares* aplicativos, *middleware* de sistema, *softwares* de faturamento, qualquer tipo de transação de comércio eletrônico, qualquer tipo de comunicações de cliente/servidor, e qualquer tipo de mensagem entre um cliente e um servidor ou onde um cliente precisa ser identificado.

Em uma forma de incorporação, dados de segurança secretos podem ser usados para prover segurança sem chave em sistemas que não usam segurança ou encriptação para as comunicações entre dispositivos de cliente e locais de internet (*websites*) ou servidores, bem como permitir a detecção de dispositivos de cliente clonados. Esta forma de incorporação é ilustrada no diagrama de fluxo da figura 7. Em uma primeira etapa

150, um dispositivo de cliente contacta um local de internet ou servidor para se registrar para um serviço. Durante a inscrição, o dispositivo de cliente envia um identificador secreto inicial ao servidor que identifica exclusivamente o dispositivo de cliente (etapa 152). O identificador secreto nesta forma de incorporação compreende uma série de valores de dados secretos, mas pode incluir uma versão transformada de tais valores em outras formas de incorporação. Os valores de dados secretos iniciais usados no identificador secreto podem ser quaisquer dados específicos de dispositivo de cliente, incluindo os dados secretos aqui descritos, que são difíceis de clonar. Ao se registrar, o cliente pode enviar uma informação de cliente um tanto difícil de clonar como identificador secreto, tal como o número de série da unidade de processamento central (UPC), se disponível, o ID de volume da unidade de disco, ou outra informação específica de *hardware*. O próprio processo de inscrição pode criar novos valores de dados secretos no lado do servidor ou no lado do cliente, que são mais difíceis de clonar, tais como dados de um ou mais registradores na UCP ou dispositivos de *hardware* de computador, o atraso de tempo em nano-segundos entre uma mensagem enviada e a resposta que é recebida pelo cliente, a soma de verificação ou valores de crc de uma porção de memória, e similares. O conjunto inicial ou tabela de dados secretos é capturado e armazenado pelo dispositivo de cliente e pelo servidor durante o processo de inscrição (etapa 154). Neste momento, os dados secreto são únicos para o dispositivo de cliente registrado, e as comunicações de cliente-servidor procedem usando o identificador secreto baseado nestes dados para validar o dispositivo de cliente (etapa 155). Neste caso, o método para detectar dispositivos de cliente clonados é aquele ilustrado na figura 4. Se o servidor recebe uma comunicação que pretende ser do dispositivo de cliente registrado mas não tem valores de dados secretos coincidindo com os valores de dados secretos iniciais armazenados no servidor para aquele dispositivo de cliente, um relatório de detecção de dispositivo clonado é gerado pelo servidor.

Como os *hackers* (piratas) podem se hábeis em piratear o sistema e obter o conjunto inicial de valores de dados

secretos, ou o identificador secreto baseado naqueles dados onde ele é transformado, novos dados secretos são criados baseado em características operacionais à medida em que o dispositivo de cliente continua operando (etapa 156). Os novos dados secretos são acrescentados ao conjunto inicial de valores de dados secretos em comunicações subseqüentes entre o servidor e o dispositivo de cliente (etapa 158), com os novos valores de dados secretos acrescentados aos valores de dados secretos previamente armazenados para aquele dispositivo de cliente (etapa 160) tanto no servidor como no dispositivo de cliente. Os novos dados secretos podem ser criados por eventos cronometrados ou eventos contados adicionando-se os dados secretos adicionais criados depois da inscrição para identificar o cliente. Opcionalmente, o servidor pode criar e distribuir dados secretos ao dispositivo de cliente em momentos variados durante a mensagem provendo o dispositivo de cliente com dados secretos adicionais que são únicos para este dispositivo de cliente. Novos dados secretos continuam sendo adicionados à medida em que o dispositivo de cliente continua operando, de modo que não há um conjunto estático de dados secretos usado para qualquer período estendido de tempo, tornando a pirataria e a clonagem muito mais difíceis. Em qualquer fase, se os dados secretos recebidos em uma mensagem de um dispositivo de cliente real pretendido não coincidirem com o conjunto atual de dados secretos armazenado para aquele dispositivo de cliente no servidor, um relatório de detecção de clone é gerado.

O método da figura 7 permite que sistemas sem segurança criem o identificadores de cliente únicos baseado em dados secretos que não podem ser pirateados facilmente. Para certas aplicações, as técnicas de dados secretos podem sozinhas prover uma segurança adequada, ou as técnicas de dados secretos podem ser acrescentadas a sistemas onde as mensagens de cliente/servidor são asseguradas usando as melhores técnicas de encriptação aperfeiçoadas com os métodos de dados secretos aqui descritos, por exemplo conforme descrito com relação às figuras 5 e 6 e Tabela 2.

As técnicas de dados secretos descritas acima podem ser usadas para aumentar a segurança quando também são usadas chaves de encriptação para encriptar mensagens entre dispositivos de computador, ou as chaves são usadas para
5 identificar seguramente computadores em uma rede. Quando um dispositivo de cliente clonado é criado, o dispositivo clonado tem as chaves idênticas de um dispositivo de cliente autorizado, autêntico ou real e pode decifrar todas as mensagens que são enviadas entre o dispositivo de cliente real autêntico autorizado
10 e o servidor. Porém, operacionalmente o dispositivo de cliente real e o dispositivo de cliente clonado executam diferentemente certas funções com o passar do tempo, ou têm valores de contagem operacionais diferentes (número de MCE processadas, momento do dia quando a 10ª mudança de canal aconteceu, e similares), de modo que
15 os dados secretos gerados pelo dispositivo de cliente real e pelo dispositivo de cliente clonado diferem, como explicado acima.

E muitos casos o valor real dos dados secretos não é importante, mas o que é importante é que o comportamento operacional de um dispositivo de cliente tal como uma caixa de
20 interface é diferente sob condições operacionais normais quando comparado a uma cópia clonada do dispositivo de cliente autêntico. Isto significa que aqueles valores de dados secretos diferem de cliente-para-cliente mesmo quando os dispositivos de cliente tiverem credenciais de cliente clonadas idênticas às do
25 dispositivo de cliente real. Em algumas formas de incorporação, estas diferenças operacionais são usadas para detectar valores de dados secretos ou identificadores secretos baseados em tais valores que diferem entre um dispositivo de cliente autêntico e um dispositivo de cliente clonado, e uma forma de incorporação de tal
30 método é explicada acima em conjunção com as figuras 5 e 6 e a Tabela 2. Além do mais, os valores de dados secretos podem ser "valores de contagem" que são pesados com um fator de escala requerendo que o dispositivo de cliente opere por um período de tempo antes que um valor mude, provendo assim valores de dados que
35 permanecem fixos em um único valor durante dias, semanas, ou meses de operação. Em uma forma de incorporação, um ou mais valores de dados secretos são utilizados como um identificador secreto nas

mensagens entre o dispositivo de cliente e o servidor. Em uma forma de incorporação, mais de um valor de dados secreto é usado com limiares ou ativadores diferentes que resultam nos vários valores de dados secretos mudando a taxas diferentes. A Tabela 4

5 abaixo mostra um exemplo de três valores ou itens de dados secretos em uma mensagem chamada de "Mensagem de Aquisição de Chave" e as mudanças nos itens de dados secretos com o passar do tempo.

A forma de incorporação das figuras 5A e 5B e

10 Tabela 2 usava uma requisição de Chave de Radiodifusão ou CRad para enviar valores de dados secretos, e as mesmas técnicas descritas abaixo na Tabela 4 para a Mensagem de Aquisição de Chave podem ser usadas no exemplo de requisição de Chave de Radiodifusão ou CRad ou quaisquer outras mensagens usadas entre um dispositivo

15 de cliente e o servidor. Note-se também que os itens ou valores de dados secretos podem se originar tanto no dispositivo de cliente, ou no servidor, ou em ambos, e que os valores de dados secretos podem ser os resultados obtidos pelo processamento de um valor de dados tal como pelo uso de uma função de *hash* (adequação de

20 dados), ou introduzindo-se um valor de número arbitrário, ou executando-se uma transformação no valor de dados usado como parte do esquema de dados secreto.

TABELA 4 - Mensagem de Aquisição de Chave (MAC) e Dados Secretos com o passar do tempo

Campos de Mensagem	Mensagem MAC após reset de acionamento	Mensagem MAC após 2 dias	Mensagem MAC após ativação da Contagem 1	Mensagem MAC após 1 semana	Mensagem MAC após 9 dias	Mensagem MAC após 2 semanas	Mensagem MAC após 3 semanas
ID de Mensagem MAC	1	1	1	1	1	1	1
Ítem 1 dos Dados Secretos	0	0	0	0	0	31	31
Ítem 2 dos Dados Secretos	0	0	0	0	88359	88359	88359

Campos de Mensagem	Mensagem MAC após reset de acionamento	Mensagem MAC após 2 dias	Mensagem MAC após ativação da Contagem 1	Mensagem MAC após 1 semana	Mensagem MAC após 9 dias	Mensagem MAC após 2 semanas	Mensagem MAC após 3 semanas
Ítem 3 dos Dados Secretos	0	0	7190	7190	RQ de 7190	RQ de 7190	RQ de 7190

O exemplo acima na Tabela 4 mostra como três valores ou ítems de dados secretos 1, 2, 3 em uma Mensagem de Aquisição de Chave (MAC) mudam com o passar do tempo. O ID de Mensagem MAC mostrado na tabela acima com um valor de "1" identifica a mensagem como sendo um Mensagem de Aquisição de Chave. É previsto que, depois de cada revisão de *firmware*, o identificador secreto que é enviado como parte das comunicações de cliente/servidor para uma função particular tal como uma requisição de aquisição de chave (ou qualquer outro evento, tal como uma transação de comércio eletrônico ou outra transação) contém ítems de dados secretos diferentes daqueles da liberação de *firmware* anterior, tornando o pirateamento de *firmware* anterior inútil no sistema. No exemplo acima, os ítems de dados secretos são valores operacionais diferentes gerados no dispositivo de cliente ou no servidor, e podem ser quaisquer dos possíveis ítems ou valores de dados secretos descritos acima, ou quaisquer outros dados únicos derivados da operação de um dispositivo de cliente. Se o servidor recebe uma mensagem de MAC a qualquer momento, a qual não coincide com a mensagem de MAC atual armazenada para o dispositivo de cliente particular, ele gera relatório de detecção de um cliente dispositivo clonado.

No exemplo acima, o ID de Mensagem para a Mensagem de Aquisição de Chave não precisa mudar e é considerado um valor de ID de Mensagem estático para indicar um dentre vários tipos de mensagem para comunicação entre o cliente e o servidor. Porém, os IDs de Mensagem podem mudar entre versões de *firmware* de cliente diferentes, forçando que os piratas (*hackers*) tenham que fazer uma "engenharia reversa" nos novos IDs de Mensagem quando uma atualização de *firmware* de cliente é feita. Um número de

revisão de *firmware* pode estar contido no ID de mensagem para permitir que o servidor trabalhe com diferentes versões de *firmware* de cliente.

Em uma forma de incorporação, os itens de dados secretos para várias liberações de *firmware* diferem entre diferentes versões. A Tabela 5 abaixo mostra uma forma de incorporação de possíveis campos de dados secretos para três liberações de *firmware* diferentes. Esta tabela mostra os conteúdos de três campos de dados secretos para três liberações de *firmware* diferentes chamadas de liberação 1.0, 1.1, e 1.2, com as várias liberações acontecendo em um período de um ano, por exemplo. Os identificadores secretos em mensagens entre dispositivo de cliente e servidor, ou servidor e dispositivo de cliente, ou ambos, consistem em três itens de dados secretos, com a natureza dos itens de dados secretos sendo dependente da liberação de *firmware* atual usada. A tabela é lida para baixo, para cada coluna. Os três itens de dados secretos para a liberação 1.0 do *firmware* são o 4º símbolo de mensagem do servidor, a contagem de pacote de MCE escalada, e o momento do dia para a terceira mensagem de um tipo particular recebida. Na liberação 1.1, estes itens mudam para uma contagem escalada do número total de horas em que o dispositivo de cliente tem operado, um símbolo recebido do servidor depois da 6ª mensagem de um tipo particular com o servidor, e o momento do dia quando a 10.000ª mensagem de um tipo particular foi recebida pelo dispositivo de cliente. Na liberação 1.2, todos os três itens de dados secretos são novamente modificados, com o item de dados secretos 2 mudado para zero, e os outros itens de dados secretos modificados para o momento do dia quando a 150ª mensagem de um tipo particular foi recebida, e o valor do número do canal no qual o dispositivo de cliente foi sintonizado às 20:37 h no dia em que o novo *firmware* foi instalado.

TABELA 5 - Exemplo de valores de dados secretos em diferentes liberações de *firmware*

Número do item de dados secretos na mensagem	Valor dos dados secretos na liberação 1.0	Valor dos dados secretos na liberação 1.1	Valor dos dados secretos na liberação 1.2
1	Símbolo recebido do servidor após a 4ª mensagem com o servidor	Contagem escalada do número total de horas em que o dispositivo de cliente tem operado	Momento do dia quando a 150ª mensagem de um tipo particular foi recebida
2	Contagem escalada de pacotes de MCE recebidos	Símbolo recebido do servidor após a 6ª mensagem com o servidor	Sempre configurado para 0 e nunca muda
3	Momento do dia quando a 3ª mensagem de um tipo particular foi recebida	Momento do dia quando a 10.000ª mensagem de um tipo particular foi recebida	Valor do número do canal que o cliente sintonizou às 20:37 h

Em uma forma de incorporação o item ou itens de dados secretos usados para qualquer liberação de *firmware* única também pode mudar em momentos pré-determinados ou em resposta a pré-determinados ativadores. Por exemplo, supõe-se que uma certa revisão de código é liberada no mês de Março e carregada no dispositivo de cliente. Durante os primeiros dois meses depois que a revisão foi carregada, o item de dados secretos 2 é o momento do dia em que o *firmware* foi atualizado. Então, depois de mais dois meses, o item de dados secretos 2 muda para um valor de dados provido pelo servidor. Então, depois de quatro meses de operação desta liberação de *firmware*, o item de dados 2 muda para o valor de registro contido em um *chip* no dispositivo de cliente no aniversário do quarto mês do carregamento da revisão. Nesta forma de incorporação, o valor de um item de dados secreto mudou três vezes durante os primeiros quatro meses de operação, de modo que os *hackers* têm mais dificuldade em clonar com sucesso o dispositivo de cliente. Quando o valor de itens de dados secretos pré-armazenados muda em uma época particular, o servidor está

atento a tal época e ajusta seu banco de dados adequadamente. Por exemplo, supondo que depois de 90 dias de operação a biblioteca de cliente é projetada para gerar uma tabela ou matriz de dados secretos completamente nova, então o servidor está atento ao fato de que depois de 90 dias de uso o cliente estará informando novos dados secretos. Na realidade, mesmo sincronizando os clones para equiparar suas velhas tabelas de dados secretos e ao mesmo tempo recarregar novos dados, isto apresenta problemas logísticos para os piratas (*hackers*), especialmente quando o *hacker* pode não estar esperando que o valores de dados secretos sejam modificados.

Há muitos itens de dados secretos e ativadores de dados secretos diferentes possíveis gerados pela operação do dispositivo de cliente, com o servidor comunicando-se com o dispositivo de cliente, ou ambos, o que pode ser usado para gerar identificadores de cliente adicionados a mensagens nas formas de incorporação acima descritas. Um ou mais itens de dados secretos podem ser um símbolo ou um tempo provido pelo servidor ao dispositivo de cliente como parte da resposta de mensagem e o item de dados provido pelo servidor é retornado de volta para o servidor pelo dispositivo de cliente (talvez na próxima requisição por um dispositivo de cliente), por exemplo como descrito acima com relação às figuras 5 e 6 e Tabela 2. Isto permite que o servidor gere símbolos usados como dados secretos para identificar clones. Dados secretos também podem ser uma contagem do número de mensagens processadas por um dispositivo de cliente ou o número de mensagens escritas para uma entrada de mensagem ou fila de mensagem pelo dispositivo de cliente, ou o valor da 10ª chamada de IPA para uma função de IPA de cliente, ou outro evento semelhante que normalmente variaria entre dispositivos de cliente mesmo com credenciais idênticas.

Em muitos casos o dispositivo de cliente pode não saber ou mesmo considerar o que significam os dados secretos, porque eles são a informação usada no lado de servidor para detectar clones, ou eram a informação provida pelo servidor para detectar clones. Em uma forma de incorporação, alguns valores de dados secretos são gerados baseado em eventos de uma só vez tal como qual canal foi sintonizado pelo dispositivo de cliente depois

de um período de tempo particular de operação de um novo dispositivo de cliente, por exemplo 23:49:33 (horas:minutos:segundos) de operação. Outros valores de dados secretos podem ser gerados usando valores operacionais de rede ou
5 de sistema tais como parâmetros de faixa de modem a cabo, tempos de arrendamento de PCHD, e similares. Ainda outros valores de dados secretos podem ser providos pelo servidor. Outros valores de dados secretos podem ser o resultado de mensagens entre um dispositivo de cliente e um servidor, ou outros parâmetros
10 normalmente encontrados no ambiente para o produto. Por exemplo, os CPs podem ter valores de dados secretos diferentes dos de telefones sem fio.

Um sistema de segurança usando dados secretos gerados por eventos operacionais de dispositivos de cliente
15 conforme descrito nas formas de incorporação acima também pode ser projetado para incluir um processo de renovação de entitulação de assinante, quando dispositivos de cliente clonados ou pirateados são detectados pelo sistema, ou são suspeitos por outras razões, ou a intervalos pré-determinados sem considerar dispositivos de
20 cliente clonados suspeitos. A figura 8 ilustra uma forma de incorporação do processo de renovação para uma rede de duas-vias ou uma rede de uma-via com um canal de retorno. Qualquer forma de canal de retorno persistente ou não-persistente (esporadicamente disponível) tal como uma conexão de discagem de modem ocasional ou
25 um canal de retorno formado quando um telefone celular é conectado a um dispositivo de cliente, tal como um STB, pode ser usado para renovação como na figura 8. Um processo semelhante também pode ser usado em uma rede de uma-via sem um canal de retorno, e uma forma de incorporação de tal um processo é ilustrado no diagrama de
30 fluxo da figura 9.

O processo da figura 8 pode ser usado em um processo de renovação com relação a redes de duas-vias ou uma rede de uma-via com um canal de retorno. Conforme ilustrado na figura 8, uma requisição para um identificador secreto é enviada por um
35 servidor em uma rede para clientes individuais (em redes de 2 vias) ou para todos os dispositivos de cliente (em uma rede de uma-via). O servidor envia uma Mensagem de Renovação ao Cliente

(181). Assumindo que um canal de retorno está disponível (182), os dispositivos de cliente são programados para responder enviando o identificador secreto atual de volta ao servidor (etapa 184). Se um canal de retorno não está disponível (isto é, o dispositivo de cliente está operando em uma rede uma-via sem canal de retorno), o procedimento continua conforme ilustrado na figura 9, e descrito em mais detalhes abaixo.

O identificador de dados secreto enviado de volta na etapa 184 para redes tendo um canal de retorno é baseado nos dados secretos coletados por um dispositivo de cliente particular, que por sua vez está relacionado a eventos operacionais naquele dispositivo de cliente. Considerando que o identificador secreto foi atualizado recentemente em cada dispositivo de cliente, os *hackers* têm que recomeçar sua pirataria para encontrar o identificador secreto do dispositivo de cliente real imediatamente depois de receber o código de atualização na etapa 179, e tentar duplicar aquele identificador secreto em qualquer dispositivo-clone. É improvável que tais tentativas de pirataria tenham êxito a tempo para que o identificador secreto seja duplicado antes que a resposta contendo o identificador secreto para cada dispositivo de cliente seja automaticamente enviado de volta de cada dispositivo de cliente na etapa 184. Em uma forma de incorporação, o identificador de dados secreto é um código de oito dígitos gerado a partir de valores de dados secretos coletados, e não contém nenhuma informação de comportamento relacionada ao assinante ou informação relacionada à privacidade. Porém, outros códigos baseados em valores de dados secretos podem ser gerados, em formas de incorporação alternativas. O servidor determina então se mais de uma resposta foi recebida com o mesmo identificador de cliente mas com dados secretos diferentes (etapa 185). Se somente uma resposta for recebida, um código de destravamento de renovação baseado no identificador secreto recebido do dispositivo de cliente é criado pelo servidor (etapa 186) e transmitido ao dispositivo de cliente (etapa 188). Se apenas uma resposta for recebida, é provável que não haja nenhum clone do dispositivo de cliente real na rede, e o dispositivo de cliente real destrava o código de renovação e é renovado para serviço. Porém, se por

alguma razão o dispositivo de cliente real não enviar uma resposta, ou os dispositivos de cliente clonados não enviarem uma resposta, mais de um dispositivo de cliente ainda pode receber o código de destravamento de renovação, já que este código é radiodifundido a todos os dispositivos de cliente que operam sob o mesmo identificador ou credenciais de cliente. Somente o dispositivo de cliente com o mesmo identificador de dados secreto pode destravar o código de renovação e ser renovado para serviços através da rede. Quaisquer outros dispositivos de cliente usando o mesmo identificador de cliente não podem destravar o código de renovação, e são bloqueados de receber serviços. Se o dispositivo de cliente renovado for de fato um clone, o assinante real é bloqueado e chama o provedor de serviço para reclamar. Neste caso, o dispositivo clonado é bloqueado e o serviço com o dispositivo de cliente do assinante real é renovado. Uma etapa opcional não mostrada na figura 8 e antes da etapa 181 seria a de enviar uma mensagem de atualização de identificador secreto ao cliente para que o cliente obtenha naquele momento ainda outros novos valores de dados secretos e os adicione à tabela de dados secretos que é retornada na etapa 184. Cada dispositivo de cliente que recebe a mensagem então atualiza o identificador secreto baseado nas características operacionais atuais do dispositivo particular para o pedaço particular de dados secretos sendo capturado.

Se mais de uma resposta de dispositivo de cliente com um identificador secreto foi recebida na etapa 185, o dispositivo de cliente real é identificado (etapa 189). A identificação do dispositivo de cliente real na etapa 189 pode incluir um método de autenticação de usuário de rede conforme descrito no pedido de patente co-pendente nº 11/489.779 depositado em 20 de Julho de 2006, seus conteúdos sendo aqui incorporados como referência. Neste método, os assinantes autorizados são associados com a locação das conexões físicas ao dispositivo de cliente, e a rede é sondada na etapa 189 para determinar qual dispositivo de cliente está na locação de rede físico correta para o assinante autorizado. Quando o dispositivo de cliente correto ou real é localizado, um código de destravamento de renovação baseado nos dados secretos recebidos daquele dispositivo de cliente é

criado na etapa 190, e é radiodifundido pela rede na etapa 192 para todos os dispositivos de cliente tendo o mesmo cliente em redes de uma só via e distribuídos unicamente a clientes em redes de duas-vias. Os serviços são bloqueados para todos os dispositivos de cliente, e somente o dispositivo de cliente real pode destravar o código de renovação e renovar os serviços.

Se o provedor de serviço não tiver procedimentos de autenticação baseados na locação física ou identificadores de conexão físico para dispositivos de cliente reais, o dispositivo de cliente real pode ser localizado através de outras técnicas, tal como por meio de uma chamada do operador de serviço ao assinante com o assinante tendo que olhar o identificador secreto no dispositivo de cliente real e prover aquele identificador ao provedor de serviço em uma mensagem de SMC ou pelo telefone.

A figura 9 ilustra etapas em um processo de renovação periódica que pode ser usado com relação a um sistema de segurança de dados secretos para dispositivos de cliente em redes de uma só via não tendo canal de retorno. Este processo de renovação usa as mesmas etapas iniciais 179, 180 e 181 conforme ilustrado na figura 8. Porém, em resposta à mensagem de renovação de código de serviço, o processador central no dispositivo de cliente é programado para exibir um código de serviço ou mensagem de renovação na tela do dispositivo de cliente (etapa 193). Esta mensagem compreende o identificador de cliente e o identificador secreto atual recuperados do módulo de armazenamento de dados secretos 29. O identificador de cliente para o dispositivo de cliente é idêntico para dispositivos de cliente reais e dispositivos de cliente clonados, mas o identificador secreto atual armazenado no dispositivo de cliente é diferente para cada dispositivo de cliente. A mensagem de código de serviço inclui uma requisição onde o usuário envia os dois IDs a um número de telefone exibido na tela, que pode ser um número 0800 para o provedor de serviço.

Na etapa 194, o usuário do dispositivo de cliente provê o identificador de cliente e ID de dados secretos para o provedor de serviço como uma mensagem de SMC para o número de telefone na tela, ou alternativamente por uma chamada telefônica

de voz para um operador no provedor de serviço. Nesta fase, o provedor de serviço pode determinar se o remetente da mensagem ou a pessoa que telefona é o assinante autorizado, baseado na informação pessoal ou informação de segurança armazenada no servidor, tal como o número de telefone do assinante autorizado. Se for determinado que a pessoa que telefonou é o assinante autorizado, o servidor ou o provedor de serviço gera um código de destravamento de renovação baseado no ID único de dados secretos recebido do usuário na etapa 195, e envia ou radiodifunde o código de destravamento de renovação a todos os dispositivos de cliente na rede com o mesmo identificador de cliente (etapa 196). Se o dispositivo de cliente que recebe o código puder processar corretamente o código de destravamento (etapa 197), o serviço é renovado para aquele dispositivo (198). Se um dispositivo de cliente que recebe o código não puder processar corretamente o código de destravamento, porque os dados secretos armazenados naquele dispositivo de cliente não coincidem com os dados secretos no código de destravamento, o serviço para aquele dispositivo de cliente é bloqueado (etapa 199). Se o sistema determinou incorretamente que a pessoa que telefonou ou remetente da mensagem requisitada é o assinante autorizado, e o usuário está realmente usando um dispositivo clonado, de modo que o dispositivo de cliente real não pode processar o código de destravamento de renovação, o usuário autorizado chama o provedor de serviço porque seu serviço foi bloqueado. Um código de destravamento de renovação adicional pode então ser gerado baseado nos dados secretos no dispositivo de cliente real e radiodifundido aos dispositivos de cliente de maneira que o dispositivo previamente renovado é bloqueado e o dispositivo de cliente real é renovado para serviço.

Os processos de renovação acima descritos com relação às figuras 8 e 9 podem acontecer a intervalos pré-determinados ou quando há suspeita da presença de um ou mais dispositivos de cliente clonados em uma rede, ou ambos. O processo de renovação conforme descrito nas figuras 8 e 9 pode usar qualquer parte das tabelas de dados secretos ou pedaços das tabelas de dados secretos para gerar códigos de destravamento específicos de dispositivos de cliente, por meio do que os

clientes clonados com valores de dados secretos diferentes não podem gerar as chaves apropriadas para decifrar o código de destravamento. Um exemplo de tal esquema de gerenciamento de chave específica de cliente é o Diffie Hellman. Outros tipos de mecanismos de troca de chave podem ser usados. Usando Diffie Hellman por exemplo, os dados secretos (quaisquer, ou todos) são usados como parte do mecanismo de introdução usado para gerar a chave única no lado do cliente ou parte dos dados usados para prover chaves compatíveis no lado do servidor de tal modo que os clientes clonados com valores de dados secretos diferentes não podem gerar a mesma paridade de chave única (paridade de chave de Diffie Hellman) entre outros dispositivos clonados. Outro modo do processo de renovação poder ser alcançado é o servidor usar os dados secretos recebidos para um cliente de um modo conhecido para introduzir ou gerar chaves de paridade compartilhadas em algoritmos tais como de Diffie Hellman, e em essência, gerar uma única paridade de chave que somente pode ser recriada pelo cliente contendo os dados secretos apropriados. Outro método opcional para executar a renovação do dispositivo de cliente é usar parte dos dados secretos como dados de chave de encriptação/decriptação porque cada cliente tem dados secretos únicos e os dados secretos únicos são conhecidos pelo servidor. Pedacos dos, ou todos os, dados secretos, ou versões transformadas ou de adequação de dados (*hashing*) dos dados secretos podem ser aplicados a chaves ou dados ou fatores de introdução usados para gerar dados de chave de encriptação/decriptação, ou usados na geração de chaves compartilhadas com algoritmos tais como de Diffie Hellman. Também é antecipado que os dados secretos podem ser usados para misturar ou transformar os dados de introdução de chave ou de fator de chave que são enviados entre o cliente e o servidor, ou servidor e cliente, durante o processo de renovação. Por exemplo, os dados secretos podem sofrer adequação (*hash*) pelo cliente e então usados como uma chave ao encriptar os dados que são enviados ao servidor. E, porque o servidor conhece os dados secretos, o servidor pode executar a mesma adequação de dados (*hash*) para gerar a chave de decriptação.

Novamente, usando Diffie Hellman como um exemplo, uma Troca de Chave de banco de dados secretos pode funcionar como se segue:

1. Alice escolhe um inteiro grande arbitrário X e
5 envia a Roberto $X = (g^x \bmod n)$ encriptado com Dados Secretos;
2. Roberto escolhe um inteiro grande arbitrário Y
e envia a Alice $Y = (g^y \bmod n)$ encriptado com Dados Secretos;
3. A Alice decifra o Y encriptado de Roberto e
computa $K = Y^x \bmod n$;
- 10 4. Roberto decifra o X encriptado de Alice e
computa $K' = X^y \bmod n$.

Depois de Diffie Hellman K e K' são iguais e os dados secretos foram usados como uma chave de encriptação para transferir dados. Os dados secretos podem ser usados em mais
15 maneiras, do que apenas na encriptação de dados de chave, e podem ser usados como dados de introdução para os cálculos de inteiros grandes arbitrários ou *hash* (adequação de dados) aplicados a dados e valores usados em cálculos de algoritmo.

Nas formas de incorporação acima, um único
20 identificador secreto é gerado baseado em eventos operacionais que acontecem durante a operação ou uso de um dispositivo de cliente, baseado em como o cliente ou o assinante usa o dispositivo de cliente. Estes eventos operacionais são diferentes entre dispositivos de cliente reais e dispositivos de cliente clonados
25 porque os dispositivos de cliente clonados são operados pelos seus usuários diferentemente de usuários de dispositivos de cliente reais ou de outros dispositivos de cliente clonados. Tais operações são extremamente difíceis de duplicar. O identificador secreto pode ser usado para detectar dispositivos de cliente
30 clonados e também em um processo de renovação periódica que pode eliminar serviços para dispositivos de cliente clonados.

Aqueles com habilidades na arte apreciarão que os vários blocos lógicos ilustrativos, módulos, circuitos, e etapas de algoritmo descritos com relação às formas de incorporação aqui
35 descritas freqüentemente podem ser implementados como *hardware* eletrônico, *softwares* de computador, ou combinações de ambos. Para ilustrar claramente esta intercambiabilidade de *hardware* e

software, vários componentes, blocos, módulos, circuitos, e etapas ilustrativas foram acima descritos geralmente em termos da sua funcionalidade. Se tal funcionalidade for implementada como *hardware* ou *software*, isto depende da aplicação particular e das

5 limitações de projeto impostas ao sistema em geral. Aqueles qualificados na arte podem implementar a funcionalidade descrita de maneiras variadas para cada aplicação particular, mas tais decisões de implementação não devem ser interpretadas como causa

10 de desvio ou fuga do escopo da invenção. Além disso, o agrupamento de funções dentro de um módulo, bloco ou etapa é para facilidade de descrição. Funções ou etapas específicas podem ser movidas de um módulo ou bloco sem haver desvio do escopo da invenção.

Os vários blocos lógicos e módulos ilustrativos descritos com relação às formas de incorporação aqui descritas

15 podem ser implementados ou executados com um processador de propósito geral, um processador de sinal digital (PSD), um circuito integrado de aplicação específica (ASIC - *application specific integrated circuit*), um arranjo de portas programáveis de campo (FPGA - *field programmable gate array*) ou outro dispositivo

20 de lógica programável, de portas discretas ou de lógica a transistor, componentes discretos de *hardware*, ou qualquer combinação relacionada projetada para executar as funções aqui descritas. Um processador de uso geral pode ser um microprocessador, mas alternativamente, o processador pode ser

25 qualquer processador, controlador, micro-controlador, ou máquina de estado. Um processador também pode ser implementado como uma combinação de dispositivos de computação, por exemplo, uma combinação de um PSD e um microprocessador, uma pluralidade de microprocessadores, um ou mais microprocessadores junto com um

30 núcleo de PSD, ou qualquer outra configuração.

As etapas de um método ou algoritmo descritos com relação às formas de incorporação aqui descritas podem ser incorporadas diretamente em *hardware*, em um módulo de *software* executado por um processador, ou em uma combinação dos dois. Um

35 módulo de *software* pode residir em uma memória RAN, memória *flash*, memória ROM, memória EPROM, memória EEPROM, em registradores, num disco rígido, num disco removível, num CD-ROM, ou qualquer outra

forma de meio de armazenamento. Um meio de armazenamento exemplificativo pode ser acoplado ao processador de tal sorte que o processador possa ler a informação do, e escrever a informação no, meio de armazenamento. Alternativamente, o meio de armazenamento pode ser integral ao processador. O processador e o meio de armazenamento podem residir em um ASIC.

Várias formas de incorporação também podem ser implementadas principalmente em *hardware* usando, por exemplo, componentes tais como circuitos integrados de aplicação específica ("ASICs"), ou arranjos de portas programáveis de campo ("FPGAs"). A implementação de uma máquina de estado em *hardware* capaz de executar as funções aqui descritas também será aparente para aqueles qualificados na arte pertinente. Várias formas de incorporação também podem ser implementadas usando uma combinação de *hardware* e *software*.

A descrição acima das formas de incorporação descritas é provida para permitir que qualquer pessoa qualificada na arte faça ou use a invenção. Várias modificações nestas formas de incorporação serão prontamente aparentes para aqueles qualificados na arte, e os princípios genéricos aqui descritos podem ser aplicados a outras formas de incorporação sem fugir do espírito ou escopo da invenção. Assim, será entendido que a descrição e desenhos aqui apresentados representam uma forma de incorporação agora preferida da invenção e são então representativos da matéria que é amplamente contemplada pela presente invenção. É compreendido adicionalmente que o escopo da presente invenção engloba completamente outras formas de incorporação que podem ser óbvias para aqueles qualificados na arte e que o escopo da presente invenção é adequadamente limitado por nada mais do que as reivindicações anexas.

R E I V I N D I C A Ç Õ E S

1. **"MÉTODO PARA SEGURANÇA DE REDE"**, caracterizado pelo fato de compreender um método de detecção de dispositivos de cliente clonados comunicando-se em uma rede, compreendendo:

5 armazenar em um servidor pelo menos um identificador secreto para um dispositivo de cliente tendo credenciais registradas em um servidor;

receber uma mensagem de um dispositivo de cliente no servidor, a mensagem contendo um identificador secreto derivado de pelo menos um evento operacional do dispositivo de cliente;

determinar se o identificador secreto recebido na mensagem coincide com um identificador secreto para o dispositivo de cliente tendo as mesmas credenciais armazenadas no servidor; e

15 reportar a detecção de um clone de um dispositivo de cliente real se pelo menos parte do identificador secreto na mensagem não coincidir com o identificador secreto armazenado para o dispositivo de cliente no servidor.

2. **"MÉTODO"**, de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto compreende valores de dados secretos selecionados gerados por eventos operacionais em um dispositivo de cliente, e a detecção de um clone de um dispositivo de cliente real é reportada se os valores de dados secretos em um identificador secreto recebido de um dispositivo de cliente não coincidem com quaisquer valores de dados secretos em um identificador secreto armazenado no servidor.

3. **"MÉTODO"**, de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto compreende um código baseado em valores de dados secretos selecionados gerados por eventos operacionais diferentes em um dispositivo de cliente.

4. **"MÉTODO"**, de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto é pelo menos parcialmente baseado em pelo menos um símbolo provido pelo servidor ao dispositivo de cliente.

5. **"MÉTODO"**, de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto é baseado em valores de dados secretos gerados pelo dispositivo de cliente.

6. "MÉTODO", de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto é baseado em dados secretos gerados pelo servidor e providos pelo servidor em uma mensagem para o dispositivo de cliente.

5 7. "MÉTODO", de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto é baseado em valores de dados secretos gerados pelo dispositivo de cliente e pelo servidor.

10 8. "MÉTODO", de acordo com a reivindicação 1, caracterizado pelo fato compreender a atualização periódica do identificador secreto em um dispositivo de cliente baseado em ativadores de eventos pré-determinados e a provisão do identificador secreto atualizado em uma mensagem para o servidor.

15 9. "MÉTODO", de acordo com a reivindicação 8, caracterizado pelo fato de que pelo menos um ativador de evento compreende a instalação de *firmware* atualizado em um dispositivo de cliente.

20 10. "MÉTODO", de acordo com a reivindicação 8, caracterizado pelo fato de que pelo menos um ativador de evento compreende a recepção de um número pré-determinado de um tipo particular de mensagem do servidor.

25 11. "MÉTODO", de acordo com a reivindicação 8, caracterizado pelo fato de que pelo menos um ativador de evento compreende enviar um número pré-determinado de um tipo particular de mensagem do dispositivo de cliente.

12. "MÉTODO", de acordo com a reivindicação 8, caracterizado pelo fato de que pelo menos um ativador de evento compreende um número pré-determinado de mudanças de canal no dispositivo de cliente.

30 13. "MÉTODO", de acordo com a reivindicação 2, caracterizado pelo fato de que a etapa de armazenar pelo menos um identificador secreto no servidor compreende armazenar um primeiro valor de dados secretos no servidor na recepção de uma pré-determinada mensagem de um dispositivo de cliente, e armazenar um
35 segundo valor de dados secretos atualizado, quando uma pré-determinada mensagem subsequente for recebida de um dispositivo de cliente tendo as mesmas credenciais, e a etapa de determinar se um

identificador secreto recebido em uma mensagem subsequente de um dispositivo de cliente coincide com um identificador secreto previamente armazenado, compreendendo comparar um valor de dados secreto na mensagem com os primeiro e segundo valores de dados secretos armazenados no servidor, por meio do que a detecção de um dispositivo de cliente clonado usando as mesmas credenciais é reportada se os valores de dados secretos na mensagem subsequente não coincidirem com pelo menos um dos primeiro e segundo valores de dados secretos.

10 14. **"MÉTODO"**, de acordo com a reivindicação 13, caracterizado pelo fato de que os valores de dados secretos são baseado no momento (tempo) de envio das mensagens pré-determinadas.

15 15. **"MÉTODO"**, de acordo com a reivindicação 13, caracterizado pelo fato de que os valores de dados secretos armazenados no servidor são baseados em valores de dados secretos recebidos em mensagens vindas de pelo menos um dispositivo de cliente.

20 16. **"MÉTODO"**, de acordo com a reivindicação 2, caracterizado pelo fato de compreender a mudança periódica de pelo menos um valor de dados secretos para um valor de dados secretos diferente baseado em um evento operacional diferente em um dispositivo de cliente.

25 17. **"MÉTODO PARA SEGURANÇA DE REDE"**, caracterizado pelo fato de compreender um método para renovar dispositivos de cliente de assinante em uma rede, compreendendo:

criar um identificador secreto em um dispositivo de cliente baseado em eventos operacionais no dispositivo de cliente;

30 receber uma mensagem de renovação de serviço no dispositivo de cliente;

prover o identificador secreto ao provedor de serviço em resposta à mensagem de renovação de serviço;

35 receber uma mensagem de código de renovação no dispositivo de cliente pela rede, a mensagem de código de renovação contendo uma código de destravamento de renovação baseado no identificador secreto; e

processar o código de destravamento de renovação usando o identificador secreto para receber serviços continuados do provedor de serviço.

18. **"MÉTODO"**, de acordo com a reivindicação 17, caracterizado pelo fato de compreender a recepção de uma mensagem de identificador secreto atualizado no dispositivo de cliente antes da mensagem de renovação de serviço, e atualização do identificador secreto no dispositivo de cliente antes de prover o identificador secreto atualizado ao provedor de serviço.

19. **"MÉTODO"**, de acordo com a reivindicação 17, caracterizado pelo fato de que o identificador secreto compreende um código baseado em valores de dados secretos selecionados gerados por eventos operacionais diferentes em um dispositivo de cliente.

20. **"MÉTODO"**, de acordo com a reivindicação 17, caracterizado pelo fato de que a etapa de prover o identificador secreto ao provedor de serviço compreende enviar o identificador secreto em uma mensagem pela rede para um servidor associado com o provedor de serviço.

21. **"SISTEMA PARA SEGURANÇA DE REDE"**, caracterizado pelo fato de compreender um sistema para detectar dispositivos de cliente clonados em uma rede, compreendendo:

um servidor tendo um módulo de comunicação que se comunica com dispositivos de cliente em uma rede;

um módulo de armazenamento de dados associado com o servidor que armazena um identificador de cliente associado com pelo menos um dispositivo de cliente real registrado para serviço com o servidor e pelo menos um identificador secreto recebido de um dispositivo de cliente tendo o mesmo identificador de cliente; e

um módulo de detecção de clone associado com o servidor e com o módulo de armazenamento de dados, que compara pelo menos um identificador secreto em uma mensagem recebida de um dispositivo de cliente com o identificador secreto armazenado associado com o mesmo identificador de cliente, e que cria um relatório de detecção de clone se o identificadores secretos não coincidirem.

22. **"SISTEMA"**, de acordo com a reivindicação 21, caracterizado pelo fato de compreender uma pluralidade de dispositivos de cliente que se comunicam com o servidor pela rede.

23. **"SISTEMA"**, de acordo com a reivindicação 22, caracterizado pelo fato de que os dispositivos de cliente são cartões inteligentes.

24. **"SISTEMA"**, de acordo com a reivindicação 22, caracterizado pelo fato de que pelo menos alguns dos dispositivos de cliente incluem cartões inteligentes.

25. **"SISTEMA"**, de acordo com a reivindicação 22, caracterizado pelo fato de que pelo menos alguns dos dispositivos de cliente são caixas de interface (STBs).

26. **"SISTEMA"**, de acordo com a reivindicação 22, caracterizado pelo fato de que pelo menos alguns dos dispositivos de cliente são dispositivos de comunicação móvel.

27. **"SISTEMA"**, de acordo com a reivindicação 22, caracterizado pelo fato de que pelo menos alguns dos dispositivos de cliente são computadores pessoais.

28. **"SISTEMA"**, de acordo com a reivindicação 22, caracterizado pelo fato de que cada dispositivo de cliente tem um módulo gerador de identificador secreto que gera um identificador secreto baseado em pelo menos um valor de dados secretos correspondendo a um evento operacional no dispositivo de cliente, um módulo de armazenamento de dados secretos que armazena valores de dados secretos, e um módulo de formatação de mensagem que embute o identificador secreto em pelo menos uma mensagem enviada ao servidor pela rede.

29. **"SISTEMA"**, de acordo com a reivindicação 28, caracterizado pelo fato de que o identificador secreto compreende pelo menos um valor de dados secreto real.

30. **"SISTEMA"**, de acordo com a reivindicação 28, caracterizado pelo fato de que o identificador secreto compreende pelo menos uma versão transformada de um valor de dados secreto.

31. **"SISTEMA"**, de acordo com a reivindicação 28, caracterizado pelo fato de que o identificador secreto compreende uma pluralidade de valores de dados secretos correspondendo a eventos operacionais diferentes no dispositivo de cliente.

32. **"SISTEMA"**, de acordo com a reivindicação 28, caracterizado pelo fato de que o identificador secreto compreende uma versão transformada de uma pluralidade de valores de dados secretos correspondendo a eventos operacionais diferentes no dispositivo de cliente.

33. **"SISTEMA PARA SEGURANÇA DE REDE"**, caracterizado pelo fato de compreender um dispositivo de cliente para se comunicar por uma rede, compreendendo:

um módulo de comunicação que se comunica com pelo menos um servidor em uma rede;

um módulo gerador de identificador secreto que cria pelo menos um identificador secreto baseado em pelo menos um valor de dados secretos de um evento operacional no dispositivo de cliente; e

um módulo de armazenamento de dados associado com o módulo gerador de dados secretos que armazena o valor de dados secretos.

34. **"SISTEMA"**, de acordo com a reivindicação 33, caracterizado pelo fato de que o dispositivo de cliente compreende um módulo formatador de mensagem associado com o módulo de comunicação e com o módulo de armazenamento de dados, que cria pelo menos uma mensagem contendo o identificador secreto para comunicação para o servidor.

35. **"SISTEMA"**, de acordo com a reivindicação 33, caracterizado pelo fato de que o módulo de armazenamento de dados armazena uma tabela de dados secretos de diferentes valores de dados secretos de eventos operacionais diferentes onde o identificador secreto é baseado na tabela de dados secretos.

36. **"SISTEMA"**, de acordo com a reivindicação 35, caracterizado pelo fato de que o identificador secreto compreende pelo menos alguns dos valores de dados secretos na tabela de dados secretos.

37. **"SISTEMA"**, de acordo com a reivindicação 35, caracterizado pelo fato de que o identificador secreto é uma transformação de pelo menos alguns dos valores de dados secretos.

38. **"SISTEMA"**, de acordo com a reivindicação 35, caracterizado pelo fato de compreender um módulo de atualização de

dados secretos configurado para atualizar a tabela de valores de dados secretos com pelo menos alguns novos valores de dados secretos em resposta a pelo menos um pré-determinado ativador de dados secretos.

5 39. **"SISTEMA"**, de acordo com a reivindicação 33, caracterizado pelo fato de que o módulo gerador de identificador secreto é configurado para gerar um identificador de cliente atualizado baseado em novos valores de dados secretos em resposta a um comando.

10 40. **"SISTEMA"**, de acordo com a reivindicação 39, caracterizado pelo fato de que o comando compreende um comando de atualização recebido em uma mensagem de rede.

 41. **"SISTEMA"**, de acordo com a reivindicação 39, caracterizado pelo fato de que o comando compreende um ativador de
15 dados secretos.

 42. **"SISTEMA"**, de acordo com a reivindicação 39, caracterizado pelo fato de compreender um módulo de renovação que responde a uma mensagem de renovação recebida de um servidor pela rede enviando um identificador secreto atual ao servidor.

20 43. **"SISTEMA"**, de acordo com a reivindicação 33, caracterizado pelo fato de compreender um cartão inteligente tendo um processador integral contendo o módulo de comunicação, o módulo gerador de identificador secreto, e o módulo de armazenamento de dados.

25 44. **"SISTEMA"**, de acordo com a reivindicação 33, caracterizado pelo fato de que o dispositivo é selecionado do grupo que consiste em caixas de interface (STBs), computadores pessoais, assistentes digitais pessoais, dispositivos de comunicação portáteis, dispositivos reprodutores de mídia, e
30 cartões inteligentes.

 45. **"SISTEMA"**, de acordo com a reivindicação 33, caracterizado pelo fato de que o dispositivo de cliente é um *chip* de silício incluindo um módulo gerador de identificador secreto e um módulo de armazenamento de dados.

35 46. **"MÉTODO"**, de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto é pelo

menos parcialmente baseado em pelo menos uma chave de encriptação provida pelo servidor ao dispositivo de cliente.

47. **"MÉTODO"**, de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto é pelo menos parcialmente baseado em pelo menos uma chave de encriptação provida pelo servidor ao dispositivo de cliente e em que o dito cliente usa a dita chave de encriptação provida pelo servidor para encriptação das comunicações entre o dito cliente e o dito servidor.

48. **"MÉTODO"**, de acordo com a reivindicação 1, caracterizado pelo fato de compreender a adição de identificadores secretos adicionais periodicamente em um dispositivo de cliente baseado em ativadores de eventos pré-determinados em que os ditos identificadores secretos adicionais são acrescentados aos prévios identificadores secretos.

49. **"MÉTODO"**, de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador secreto é baseado no tempo (momento) do dia em que um evento aconteceu no dispositivo de cliente.

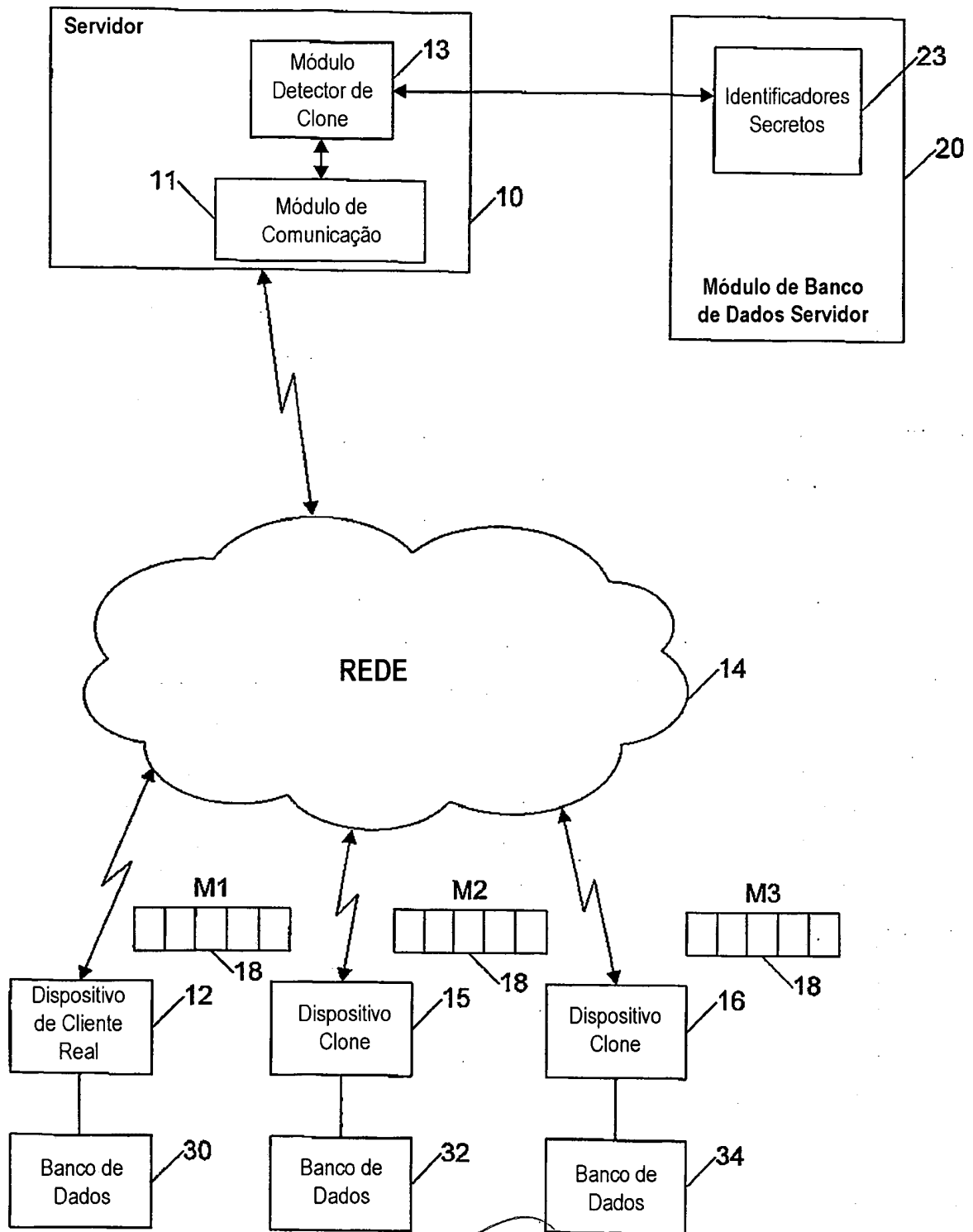
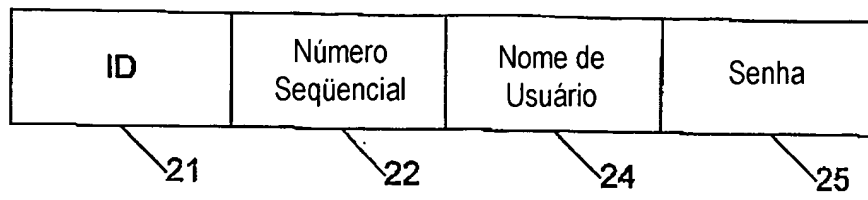
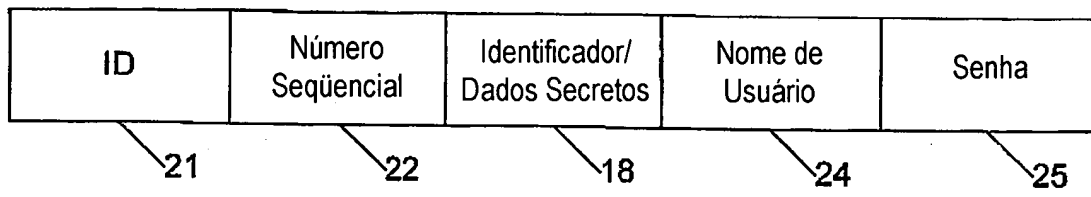


FIG. 1

**FIG. 2A****FIG. 2B**

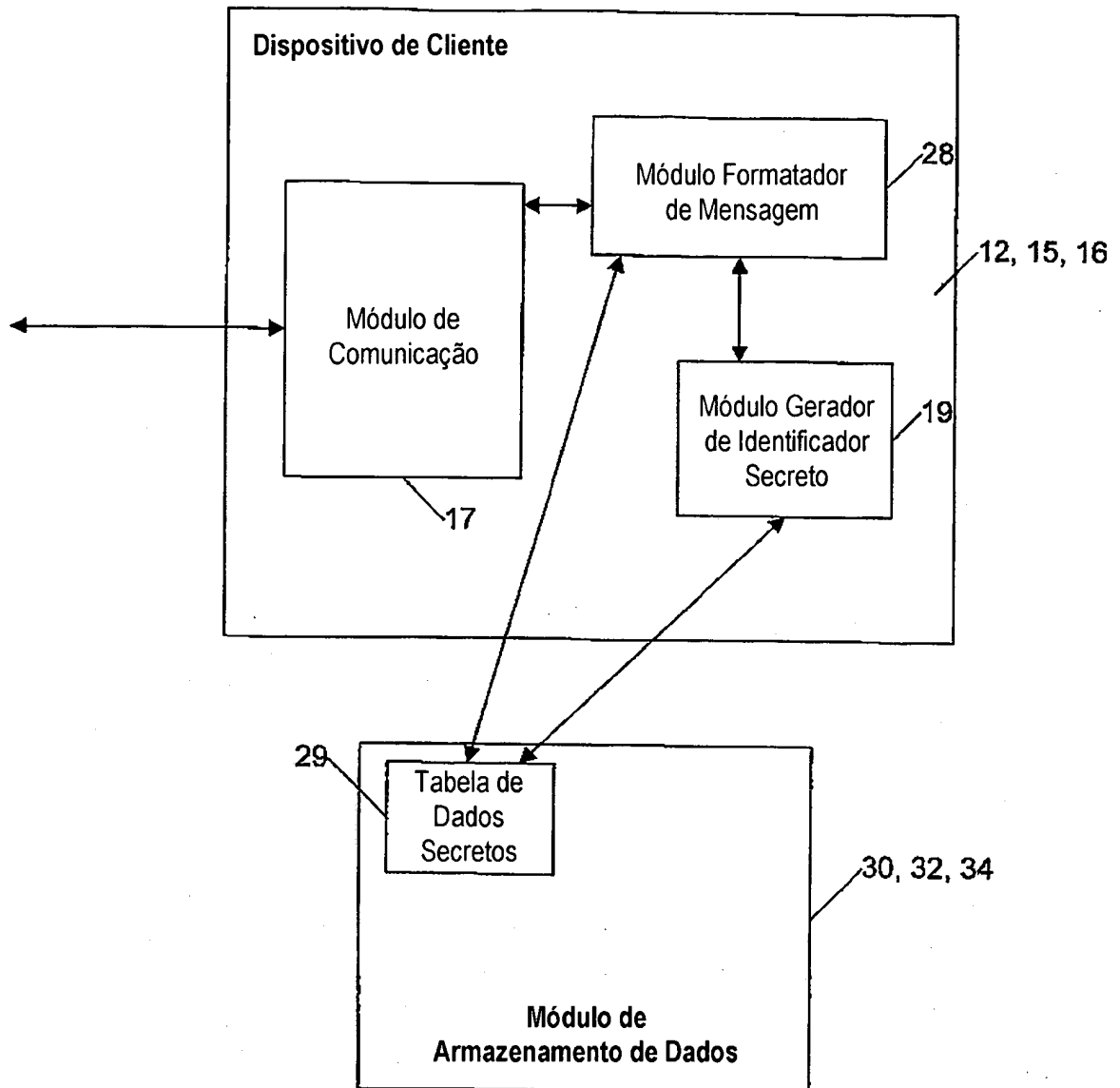
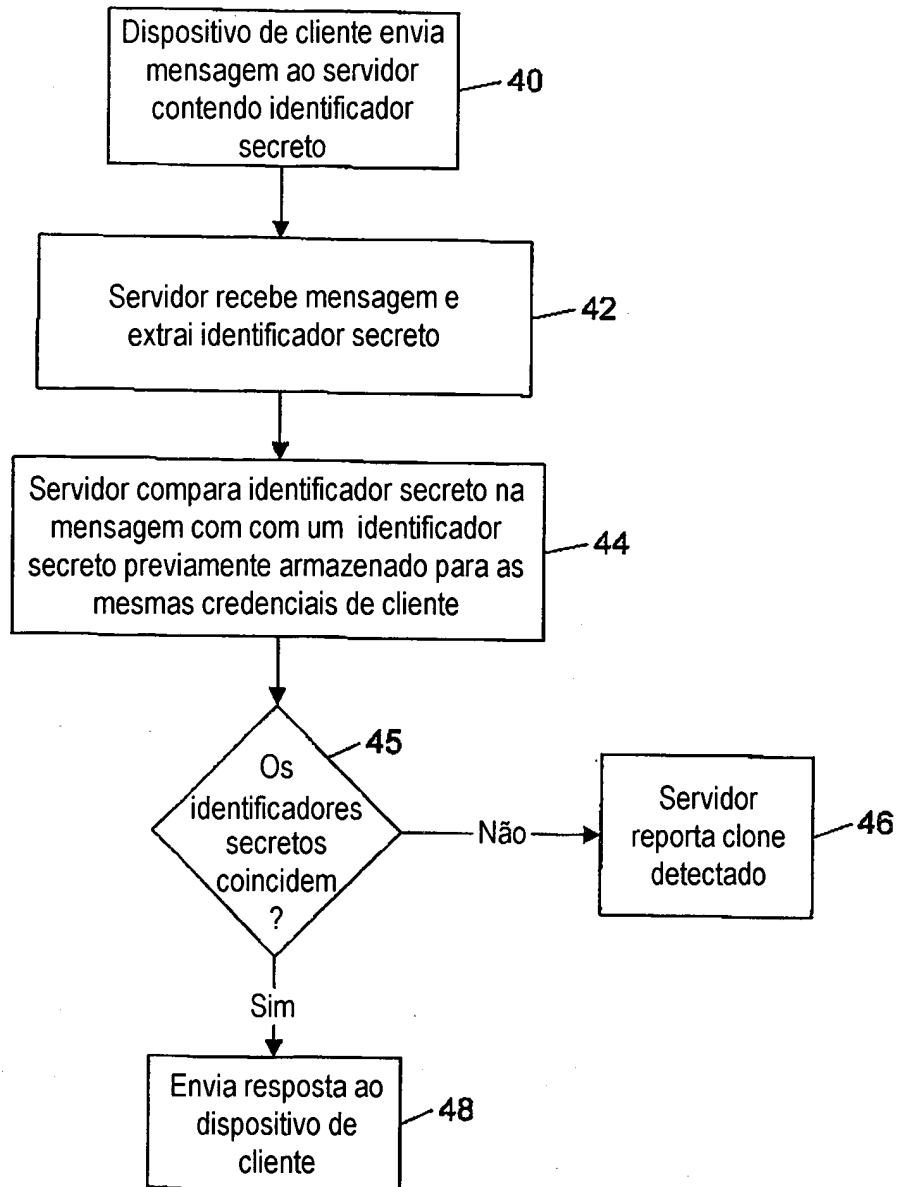


FIG. 3

**FIG. 4**

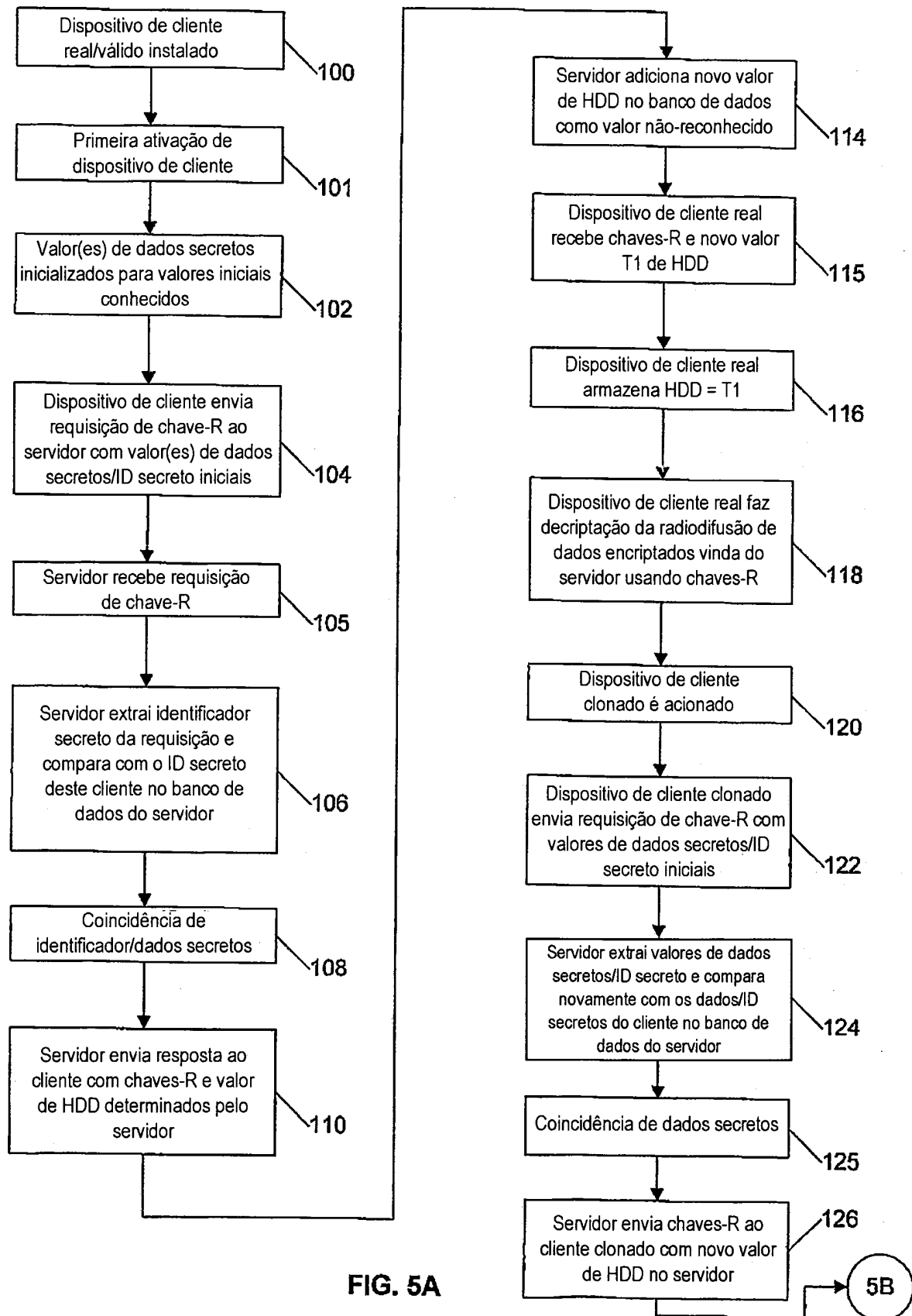


FIG. 5A

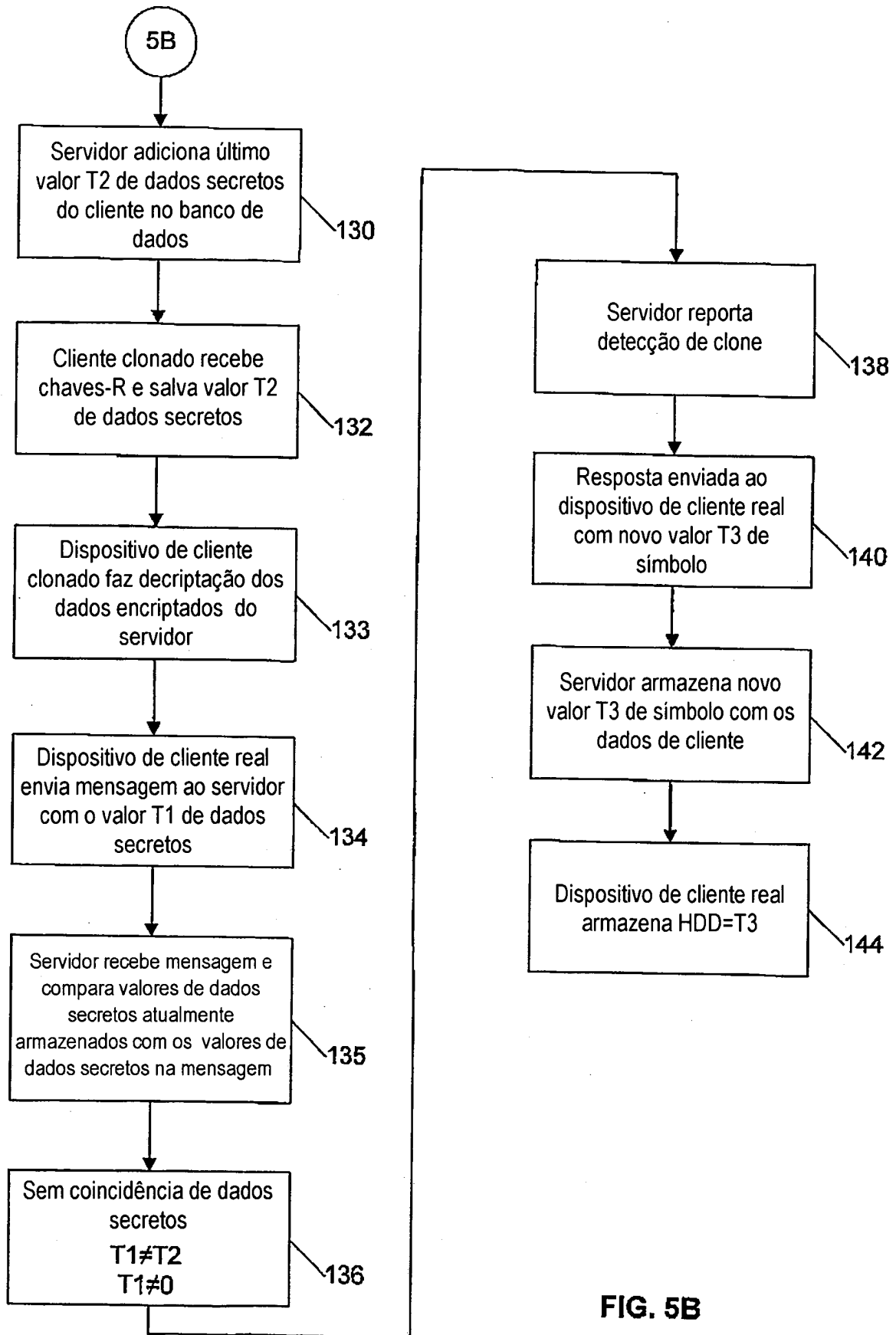
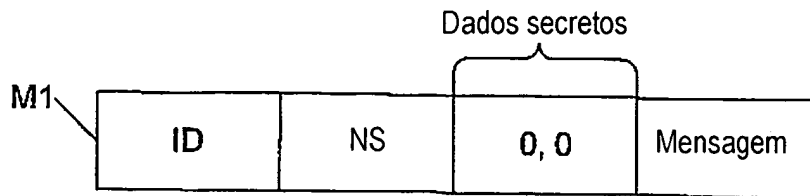
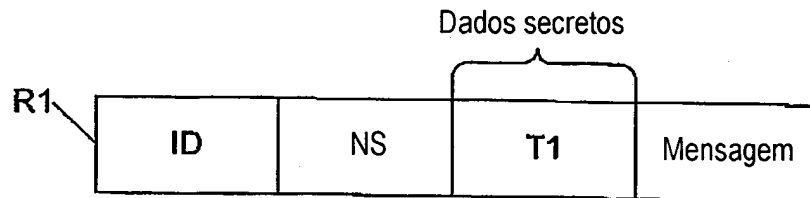
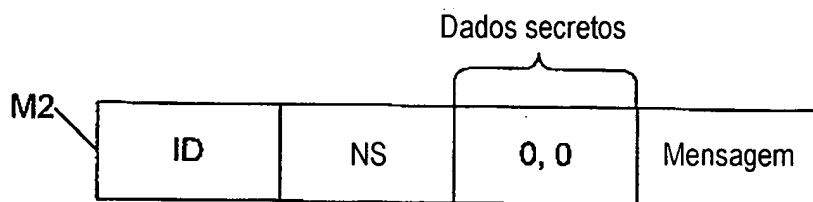
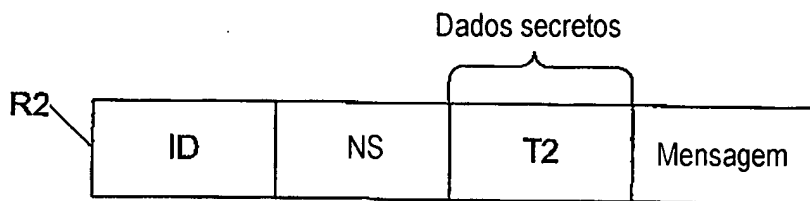
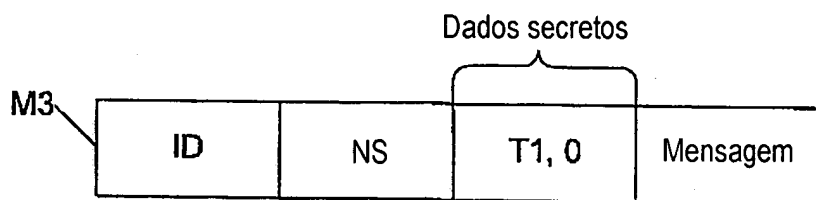
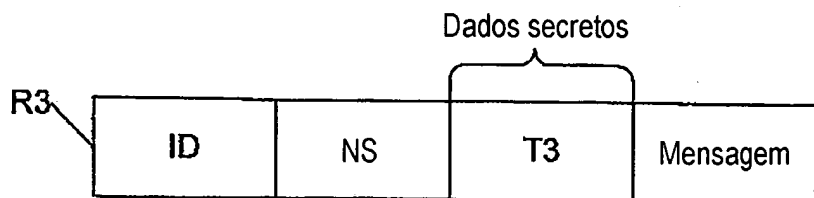


FIG. 5B

**FIG. 6A****FIG. 6B****FIG. 6C****FIG. 6D****FIG. 6E****FIG. 6F**

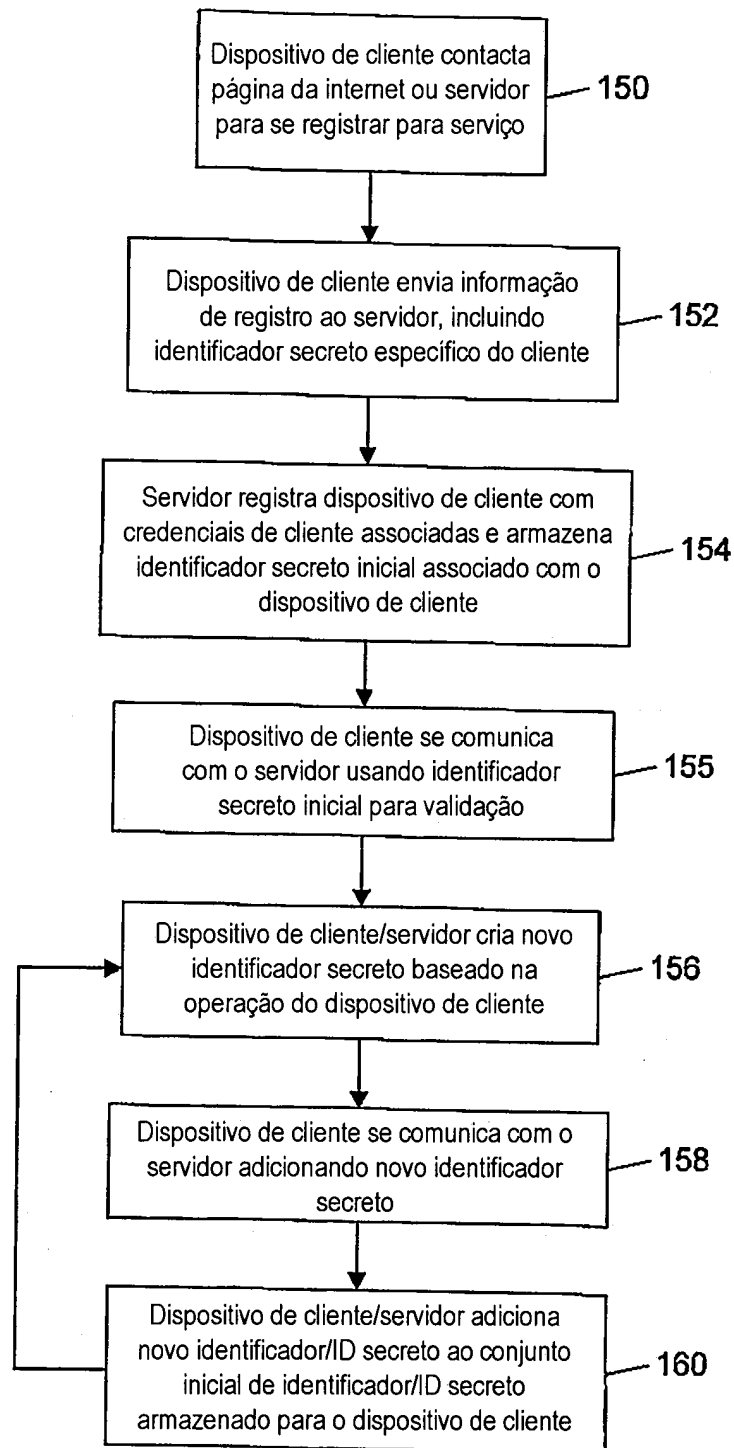


FIG. 7

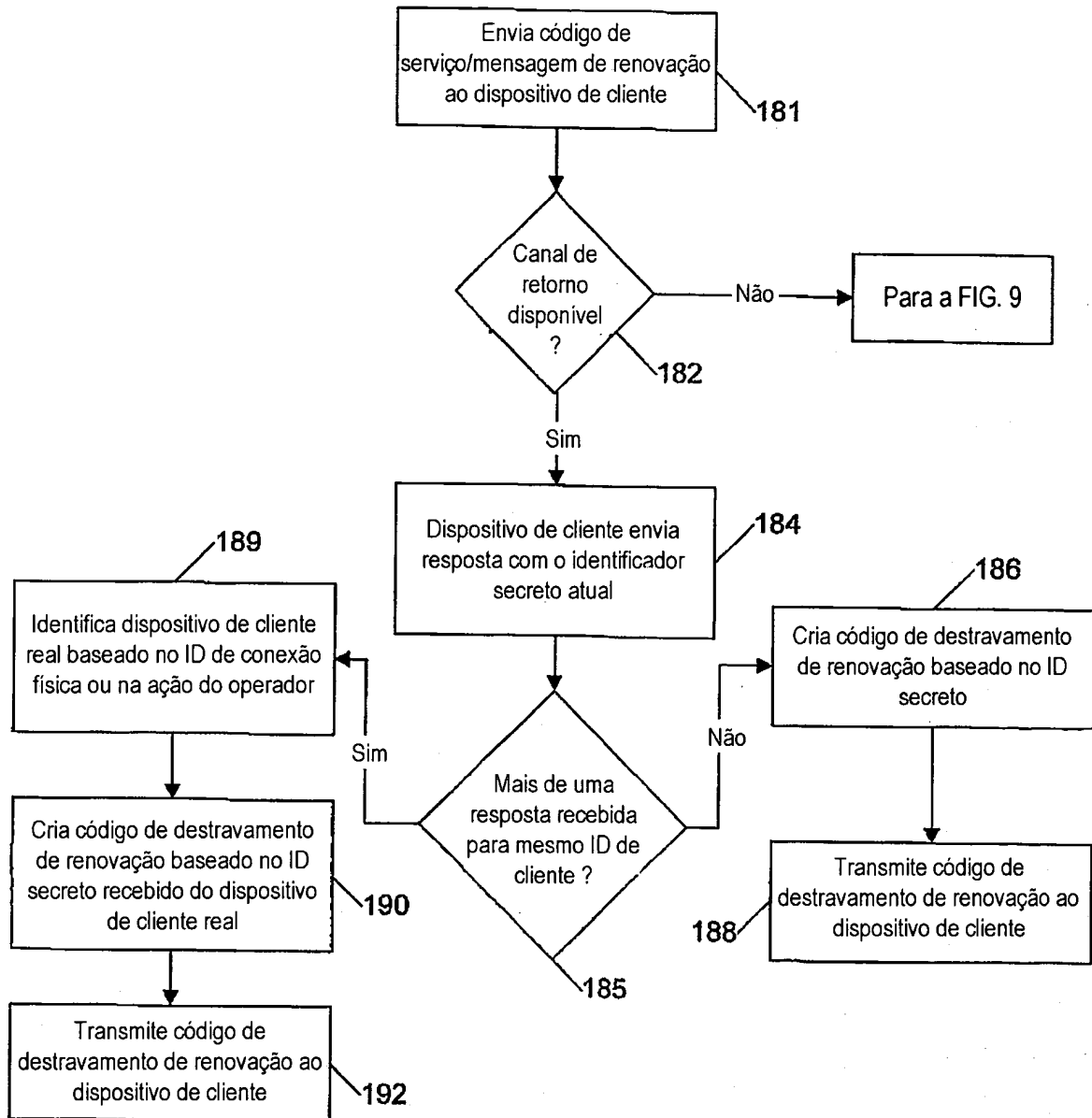


FIG. 8

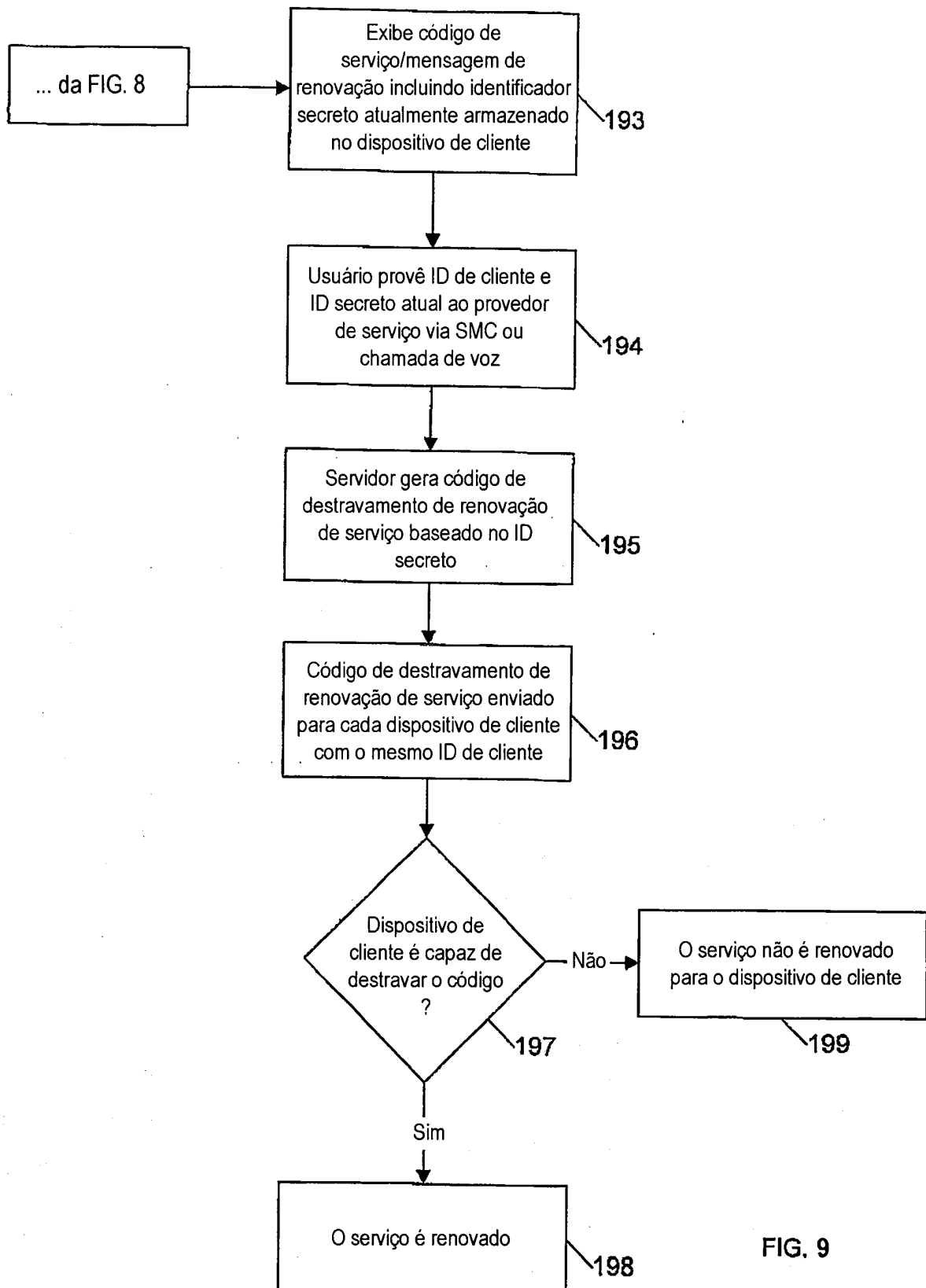


FIG. 9

R E S U M O**"SISTEMA E MÉTODO PARA SEGURANÇA DE REDE"**

Em um sistema de segurança para comunicações de rede com dispositivos de cliente, cada dispositivo de cliente tem

5 um módulo de comunicação para se comunicar com pelo menos um servidor em uma rede, um módulo de armazenamento de dados para armazenar um ou mais valores de dados secretos de um ou mais eventos operacionais no dispositivo de cliente, e um módulo gerador de identificador secreto que cria pelo menos um

10 identificador secreto baseado nos valores de dados secretos armazenados. O identificador secreto é provido em uma ou mais mensagens de rede ao servidor, ou caso contrário enviadas ao provedor de serviço, e pode ser provido em resposta a uma requisição específica recebida na rede, ou habitualmente em uma ou

15 mais mensagens normalmente envolvidas em comunicações de rede. O servidor compara os identificadores secretos recebidos de dispositivos de cliente tendo o mesmo identificador de cliente para detectar possíveis clones.